Ministerie van Defensie

Toezichtjaarverslag 2021

Functionaris voor Gegevensbescherming

Colofon

Toezichthouder
Functionaris voor Gegevensbescherming

Adres
Plein Kalvermarkt Complex
Kalvermarkt 32
Postbus 20701
2511 CB Den Haag
Bezoekadres: Plein Kalvermarkt

Datum
Maart 2022

Inhoudsopgave

Voorwoord

De Functionaris voor Gegevensbescherming (FG) ook wel aangeduid als Data Protection Officer (DPO), is bij het ministerie van Defensie de interne toezichthouder die toeziet op de naleving van de wet- en regelgeving rond de bescherming van de persoonlijke levenssfeer, ten aanzien van de verwerking van persoonsgegevens. De Algemene verordening gegevensbescherming (Avg), de Uitvoeringswet Avg (Uavg) en de Wet politiegegevens (Wpg) zijn hiervoor de wettelijke basis.

Digitalisering, een informatiegestuurde krijgsmacht, cyberveiligheid en daarmee ook privacy staan als onderwerpen hoog op de maatschappelijke en politieke agenda. Binnen Defensie is de opkomst zichtbaar van technologische toepassingen voor biometrische herkenning, verwerking van DNA en het monitoren van prestaties en gezondheidsaspecten. Met de coronapandemie zijn daar in 2021 ook vraagstukken bijgekomen rond gezondheidsmonitoring.

De Defensievisie 2035 *Vechten voor een veilige toekomst* onderkent het belang van informatiegestuurd organiseren in optreden en onderstreept dat Defensie ook toegerust moet zijn om, binnen de geldende ethische en juridische kaders, op te treden in de informatieomgeving. Rechtmatig en zorgvuldig omgaan met persoonsgegevens wordt steeds belangrijker. Implementatie van gegevensbescherming beperkt zich daarbij niet alleen tot bedrijfsvoeringsprocessen, maar richt zich ook op operationele processen.

De komende jaren is het van belang om alle bestaande en nieuwe processen verwerkingsactiviteiten waarbij verwerkingen van persoonsgegevens plaatsvinden steeds zorgvuldig te inventariseren en te beoordelen, zodat Defensie voor alle verwerkingen ‘compliant’ en ‘in control’ is. Een belangrijk hulpmiddel daarbij zijn de Data Protection Impact Assessments (DPIA’s), die in veel gevallen op systeem- of proces, maar soms ook al op beleidsniveau uitgevoerd dienen te worden.

Een verdergaande professionalisering en versterking van de Avg-/Wpg-organisatie is noodzakelijk. Door actief FG-toezicht wordt het belang van een professionele inrichting van de Avg/Wpg-organisatie in toenemende mate door de defensieorganisatie onderkend. De vooruitzichten zijn positief. Het toezicht heeft de afgelopen jaren bijgedragen aan een groter gevoel van urgentie op het gebied van gegevensbescherming binnen Defensie. Structurele inbedding van privacygovernance, meer aandacht voor Avg-/Wpg-compliance en zicht op voldoende (kwalitatieve) capaciteit om de Avg-/Wpg-organisatie te professionaliseren, heeft de aandacht van de defensieorganisatie.

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

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

Leeswijzer

Dit verslag vindt zijn grondslag in artikel 38 lid 3 van de Avg en artikel 1.5, lid 3 van de Regeling Avg Defensie (Besluit 15 mei 2018, Staatscourant 2018, nr. 28291) en in artikel 36 lid 4 Wpg en artikel 1.6 lid 3 van de regeling Wpg Defensie (Besluit 16 december 2018, Staatscourant 2018, nr. 72552, laatstelijk gewijzigd bij besluit van 8 november 2019 Staatscourant 2019, nr. 62419). Hierin is bepaald, dat de FG's jaarlijks hun bevindingen rapporteren over de naleving van de Avg, de Uitvoeringswet Avg en de Wpg binnen het Ministerie van Defensie. In de SG-Aanwijzing 948 "Toezicht bij Defensie" is voorgeschreven, dat de FG jaarlijks, uiterlijk op 15 maart het jaarverslag opstelt. Met dit Toezichtjaarverslag wordt invulling gegeven aan de rapportageverplichtingen over het jaar 2021.

In hoofdstuk 1 en 2 staan het toezicht in 2021 centraal en worden de hoofdlijnen uit het toezicht besproken. Dit geeft een terugblik op het toezichtjaar, hierin worden de herprioriteringen en de invloed van de coronapandemie op de toezichtsactiviteiten benoemd. Tevens wordt de samenwerking binnen en buiten defensie belicht. De uit het jaarrapport naar voren gekomen belangrijke conclusies en aanbevelingen voor de bevordering van de naleving van de wetgeving op het gebied van privacy- en gegevensbescherming worden in hoofdstuk 1.2 onder elkaar gezet

In hoofdstuk 3 van dit Toezichtjaarverslag wordt aan de hand van het wettelijk normenkader gerapporteerd in hoeverre de Avg- en Wpg-(onder)beheerders de passende technische en organisatorische maatregelen hebben getroffen, om te waarborgen en aan te kunnen tonen dat verwerkingen van persoonsgegevens binnen Defensie in overeenstemming met de Avg en Wpg zijn. Over de naleving in 2021 wordt in dit hoofdstuk aan de hand van deze basisnorm, per Avg- of Wpg-(onder)beheerder, over elk defensieonderdeel gerapporteerd. Hierdoor ontstaat een duidelijk overzicht van de stand van zaken bij Defensie, de mate van naleving en de aandachts- en verbeterpunten. Doordat telkens hetzelfde normenkader wordt gehanteerd, bieden de opeenvolgende jaarverslagen een meerjarig beeld.

1 Toezicht 2021

1.1 Inleiding

In het Toezichtjaarplan 2021[1] werden, naast het lopende toezicht, de speerpunten en prioriteiten voor 2021 beschreven. Kort na het vaststellen van het Toezichtjaarplan berichtte het NRC Handelsblad over de activiteiten van het Land Information Manoeuvre Centre (LIMC). Daarop is door de FG op 18 november 2020 een ad hoc toezichtbezoek aangekondigd en uitgevoerd, gevolgd door een onderzoek naar de naleving van de Avg bij de verwerkingen van persoonsgegevens door de Experimenteeromgeving LIMC. Op 31 maart 2021 kwam het FG onderzoeksrapport over LIMC uit, getiteld 'Onderzoek naleving Algemene verordening gegevensbescherming Experimenteeromgeving Land Information Manoeuvre Centre (LIMC)'.

Halverwege 2021 is, naar aanleiding van het LIMC-onderzoek, door de FG een vervolgonderzoek ingesteld naar de manier waarop zogenoemde social monitoring tools worden gebruikt bij de defensieonderdelen.

De uitvoering van het LIMC-onderzoek vroeg veel tijd en aandacht in de eerste helft van 2021. Het onderzoek naar het gebruik van social monitoring tools bij de defensieonderdelen begon in de tweede helft van 2021 en wordt naar verwachting in de eerste helft van 2022 afgerond.

Behalve voor het onderzoek zelf was veel FG-capaciteit nodig voor de politiek bestuurlijke processen rond het LIMC-onderzoek. Dit betrof onder meer het informeren van de politieke en ambtelijke top over de conclusies en adviseren over de opvolging van de aanbevelingen, het gezamenlijk met de CDS verzorgen van een Technische Briefing, vragen en –moties uit de Tweede Kamer en afstemming met de Autoriteit Persoonsgegevens.

Vanwege de beperkt resterende toezichtscapaciteit en onder invloed van de beperkingen door Corona werden in 2021 vrijwel geen reguliere planbare toezichtbezoeken uitgevoerd.

Samenvattend lag in 2021 voor het nalevingstoezicht met name de nadruk op de uitvoering van het LIMC-onderzoek en het opstarten van het vervolgonderzoek social monitoring tools. Daarnaast is ingezet op het uitvoeren van het reguliere systeemgericht en kwaliteitstoezicht.

Het systeemgericht- en kwaliteitstoezicht, uitgevoerd in samenwerking met de Avg-coördinatoren en Wpg-privacyfunctionaris, richt zich op het monitoren van de kwaliteit en de naleving en het op basis van de wettelijke normen in kaart brengen en beoordelen of er voldoende en passende technische en organisatorische maatregelen zijn getroffen om te waarborgen en aan te tonen dat de verwerkingen van persoonsgegevens binnen Defensie in overeenstemming met de Avg en Wpg uitgevoerd worden.

In 2021 nam in het systeemgericht en kwaliteitstoezicht de rol van de FG vooral toe bij de uitvoering en appreciatie van Data Protection Impact Assessments (DPIA).

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 de risico's te verkleinen. Als er onvoldoende zekerheid kan worden geboden dat de verwerking in overeenstemming is met de Avg of de Wpg, dan kan de verwerking niet aanvangen of worden voortgezet. In uitzonderlijke gevallen dient te worden overwogen bij de externe

[1] BS2020023831, Toezichtjaarplan Functionaris Gegevensbescherming 2021, 20 november 2020

toezichthouder, de Autoriteit Persoonsgegevens, het traject van voorafgaande raadpleging te doorlopen.

Er is een sterke toename zichtbaar in het aantal uit te voeren DPIA's en ook de complexiteit neemt toe. Het verplichtende karakter van de DPIA 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 als proceseigenaar of verantwoordelijke beleidsdirectie.

Positief gevolg van de media-aandacht rond het LIMC-rapport is dat binnen Defensie het bewustzijn is toegenomen over het belang van naleving van de privacywetgeving. Binnen Defensie droegen in 2021 diverse activiteiten bij aan het verhogen en scherp houden van het privacybewustzijn. Op initiatief van CLSK werd bijvoorbeeld gewerkt aan een defensiebreed initiatief genaamd 'Data Deletion Day'. Ook werden defensiebreed workshops en trainingen gegeven. De belangrijkste waren de Masterclasses DPIA, die in het derde en vierde kwartaal georganiseerd werden. Hieraan hebben in totaal circa 100 defensiemedewerkers deelgenomen. De jaarlijkse 'week van privacy en beveiliging' kon in 2021 door andere prioritering van werkzaamheden en door de coronabeperkingen helaas niet doorgaan.

1.2 Reflectie Toezicht 2021

De FG signaleert dat de structurele inbedding van privacygovernance en risicomanagement bij Defensie nog volop in ontwikkeling is. Defensie heeft maatregelen getroffen die bijdragen aan de beheersing van de privacyrisico's teneinde de naleving van de Avg en Wpg te borgen. De taken, verantwoordelijkheden en rapportagelijnen rond de Avg en de Wpg zijn vastgelegd en grotendeels ingericht conform het beleid. De Avg/Wpg-organisatie is grotendeels ingevuld. Er is een register van verwerkingsactiviteiten om inzicht te geven in welke verwerkingen van persoonsgegevens er binnen Defensie plaatsvinden.

Door beleidsinitiatieven, technologische ontwikkelingen en een toenemend privacybewustzijn nemen kansen voor privacy en risico's op privacyschendingen toe. Privacy is niet alleen een last, maar ook een lust. Het is een grondrecht om na te leven; juist in het huidige digitale tijdperk. Voldoende capaciteit en middelen om daarmee de Avg-/Wpg-functie te professionaliseren zijn daarbij essentieel. Dit heeft door actief FG-toezicht ook de benodigde aandacht van de defensieonderdelen.

Meer aandacht is nodig voor de systematische borging van Avg- en Wpg-compliance binnen de defensieorganisatie, verhoogde 'privacy awareness' en verhoging van de kwaliteit van de DPIA's en van de registraties in het register van verwerkingsactiviteiten. Voldoende capaciteit en middelen om daarmee de Avg-/Wpg-functie te professionaliseren zijn daarbij essentieel. De professionalisering van de Avg-/Wpg-functie en de intensivering van de samenwerking met de juridische en operationele lijn is daarbij van belang.

De top drie aanbevelingen voor de bevordering van de naleving van de wetgeving op het gebied van privacy- en gegevensbescherming zijn:

Aanbeveling 1 :

Versterk en professionaliseer de Avg coördinatiefunctie en intensiveer de samenwerking met de juridische en operationele lijn. Investeer in het vergroten van capaciteit en kennisniveau, zowel kwantitatief en kwalitatief waar noodzakelijk.

Aanbeveling 2:

Besteed meer aandacht voor de beveiliging van persoonsgegevens bij de uitwisseling ervan met externe partijen en investeer in het verhogen van de bewustwording (behoeftestellers & inkoopketen).

Aanbeveling 3:

Verhoog de kwaliteit van DPIA's en registraties in het register van verwerkingsactiviteiten. Completeer en documenteer het Defensie verwerkingenregister (inclusief DPIA's en verwerkersovereenkomsten).

1.3 Invloed coronapandemie

Door de coronamaatregelen is, net als in 2020, ook in 2021 besloten om nagenoeg geen fysieke toezichtbezoeken af te leggen tenzij dit in het belang van het onderzoek onvermijdelijk was.
Waar mogelijk zijn interviews en gesprekken ten behoeve van het toezicht digitaal afgenomen.
De genoemde maatregelen hebben de werkzaamheden ook in 2021 bemoeilijkt. Enkele voorbeelden:

- Fysiek overleg en toezichtbezoeken op defensielocaties waren zeer beperkt mogelijk. Bij toezicht op afstand, door middel van videovergaderingen en digitale uitwisseling van documenten, vragen en antwoorden, werden het gebrek aan interactie en persoonlijk contact en het lastiger kunnen vormen van een inzicht van de praktijk als belangrijke nadelen ervaren. Hierdoor werd de effectiviteit van het toezicht minder.
- (Internationale) Kennis- en netwerkbijeenkomsten werden in 2021 digitaal gehouden; onderlinge samenwerking en verbinding kwam daardoor lastiger tot stand.
- In 2021 konden nieuwe en tijdelijke medewerkers bijna uitsluitend op afstand via digitale middelen ingewerkt worden. Voor hen is het leren kennen van Defensie en een netwerk opbouwen bij Defensie lastiger. Ook voor teambuilding en groepsgevoel zijn fysieke contactmomenten noodzakelijk.

2 Hoofdlijnen uit het toezicht

De defensieorganisatie richt zich continu op de ontwikkeling en toepassing van nieuwe en innovatieve werkwijzen en het optimaliseren van bestaande processen. Technologische en organisatorische ontwikkelingen doen zich defensiebreed voor, zowel in de bedrijfsvoeringsprocessen als in de operationele taakuitvoering. De digitalisering van de sensor-, wapen- en commandosystemen neemt toe. Schepen, vliegtuigen en voertuigen krijgen steeds meer slimme sensoren en ICT toepassingen aan boord. In 2021 kwamen ook in de bedrijfsvoering nieuwe ontwikkelingen op het gebied van informatievoorziening en ICT naar voren, bijvoorbeeld in verband met de coronapandemie. Voorbeelden zijn cloud- en vergaderdiensten, die plaats- en tijdonafhankelijk werken faciliteren, of verwerking van gezondheidsgegevens in verband met het tegengaan van coronabesmettingen.

Het gaat om uiteenlopende producten, diensten en applicaties waarbij gebruik wordt gemaakt van nieuwe technologieën. Voorbeelden hiervan zijn het ontwikkelen van business intelligence dashboards, de toepassing van kunstmatige intelligentie (AI), algoritmes, slim cameratoezicht, gezondheidsmonitoring en biometrische sensoren. Ook komen er, in het kader van het informatiegestuurd optreden, steeds meer tools beschikbaar die informatie en datastromen verwerken en inzichtelijk maken. Hierbij kan het ook gaan om informatie uit openbare en vrij toegankelijke bronnen, zoals het internet, 'internet-of-things' en elektromagnetisch spectrum-analyse (bijvoorbeeld wifi-tracking).

Bij een groot deel van de nieuwe middelen, systemen, producten en diensten die Defensie ontwikkelt en inkoopt, gaat het om hoogtechnologische-, sensorische- en data gedreven toepassingen. Defensie beschikt hiermee over steeds grotere hoeveelheden data die persoonsgegevens bevatten en daar zitten ook vaak gevoelige en bijzondere persoonsgegevens bij.

Bewust of onbewust misbruik of onverantwoordelijk gebruik van deze technologieën kan leiden tot onrechtmatige gegevensverwerkingen, onjuiste besluitvorming, discriminatie en uitsluiting of veiligheidsrisico's, zoals datalekken.

In 2021 is een verhoging en een verschuiving van de werk- en toezichtdruk in het werkveld van privacy- en gegevensbescherming zichtbaar. Zowel in de bedrijfsvoeringsprocessen als in de operationele taakuitvoering is meer aandacht gevraagd voor de zorgvuldige en rechtmatige verwerking van persoonsgegevens. De privacywetgeving vereist immers dat de toezichthouder zich extra richt 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. Daarbij is het in veel gevallen noodzakelijk om voor aanvang van de verwerking een gedegen en volledige gegevensbeschermingseffectbeoordeling (GEB ofwel DPIA) uit te voeren.

2.1 Herprioriteringen

Incidentonderzoeken naar mogelijke onregelmatigheden in verband met persoonsgegevens en inbreuken op de beveiliging (datalekken) zijn in 2021 toegenomen, onder meer in verband met de verwerking van persoonsgegevens betreffende de gezondheid. Er is een toename in het aantal uit te voeren en door de FG te appreciëren DPIA's te zien. Eind 2020 werd een

omvangrijk toezichtonderzoek geïnitieerd naar de naleving van de Avg, in relatie tot de verwerkingsactiviteiten van de experimenteeromgeving Land Information Manoeuvre Centre (LIMC) binnen de Koninklijke Landmacht. Dit onderzoek is op 31 maart 2021 afgerond met een rapportage die op 19 april door het onderzoeksteam is aangeboden aan de Secretaris-Generaal en de Minister van Defensie als verwerkingsverantwoordelijke. Het onderzoek heeft veel capaciteit gekost en was mede de aanleiding tot een breed vervolgonderzoek naar het gebruik van social monitoring tools binnen Defensie.

2.2 Ontwikkelingen in het domein gegevensbescherming

Rechtmatig en zorgvuldig omgaan met persoonsgegevens wordt steeds belangrijker. Defensie werkt aan verdergaande digitalisering en doorloopt een transitie naar informatiegestuurd optreden, zowel in de bedrijfsvoering als in de operationele taakuitvoering.

"We moeten ons voorbereiden op een combinatie van minder personeel en meer technologie, waardoor er méér wordt bereikt.

Voor mij zijn er vier focuspunten bij de transformatie. Die staan overigens niet op zichzelf, maar grijpen in elkaar en versterken elkaar.

Het zijn:
Schaalbare eenheden;
Multidomein optreden;
Informatiegestuurd en gedigitaliseerd;
en tot slot
Samen met partners."

Over de focuspunten informatiegestuurd en gedigitaliseerd:

"Binnen de strategische competitie vormt digitalisering de rode draad. Data vormt de basis voor onze bedrijfsvoering en onze operaties.
Dat vraagt om moderne en veilige communicatiemiddelen en IT, zowel in Nederland als voor ons optreden wereldwijd. Op het slagveld kunnen onze mensen het verschil maken, omdat zij naast de menselijke kant nog een andere kant bij of in zich hebben: de kant van de data. Data die werkt vóór hen. Die hen voorsprong geeft in de strategische competitie en hen het vermogen geeft om levensbepalende keuzes te maken.
Data werkt dus samen met en voor onze mensen. Het is een doel, een middel en een wapen. Het maakt ons sneller, slimmer en sterker.
En daar hoort ook Command en Control bij.

Digitalisering en multidomein optreden met schaalbare eenheden zorgen voor een andere inrichting van onze krijgsmacht."

Bron *Commanders Intent Commandant der Strijdkrachten 8 oktober 2021, Defensietop-dag te Stroe*

De Defensievisie 2035 *Vechten voor een veilige toekomst* onderkent het belang van informatiegestuurd organiseren in optreden, en onderstreept dat Defensie ook toegerust moet zijn om, binnen de geldende ethische en juridische kaders, op te treden in de informatieomgeving. In het kader van de uitvoering van de politietaken voert de Koninklijke Marechaussee het programma IGO uit en heeft vanaf 2015 definitief de transitie ingezet van een gebiedsgebonden-oriëntatie naar een landelijke centrale informatiegestuurde organisatiestructuur.

In lijn met deze visie en ambities en de daaruit voorvloeiende ontwikkelingen groeit het belang van goede toepassing van gegevensbescherming, informatievoorziening en informatiebeveiliging. Dit vereist eveneens een groei van de benodigde capaciteit en middelen voor het beleid, de uitvoering en het toezicht op gegevensbescherming.

Door beleidsinitiatieven, technologische ontwikkelingen en een toenemend privacybewustzijn nemen kansen voor privacy en risico's op privacyschendingen toe. Voldoende capaciteit en middelen om daarmee de Avg- en Wpg-functie te professionaliseren en intensivering van de samenwerking met de juridische en operationele lijn zijn essentieel. Meer aandacht is nodig voor opleiding en een systematische borging van Avg- en Wpg-compliance binnen de defensieorganisatie, waarbij aandacht wordt gevraagd voor inbedding in het reguliere risicomanagement en de verhoging van de kwaliteit van de DPIA's en de registraties in het register van verwerkingsactiviteiten.

2.3 Samenwerking

Bij Defensie zijn verschillende toezichthouders actief. Samen controleren zij op thema's zoals gezondheidszorg, (vlieg)veiligheid, beveiliging, voedselveiligheid, stralingsbescherming en de bescherming van persoonsgegevens. De toezichthouders zijn: de Inspectie Veiligheid Defensie (IVD), de Inspectie Militaire Gezondheidszorg (IMG), het Korps Militaire Controleurs Gevaarlijke Stoffen (KMCGS), de Militaire Luchtvaart Autoriteit (MLA), de Directeur Bedrijfsvoering en Evaluatie in zijn rol als Beveiligingsautoriteit (BA) en de Functionarissen voor Gegevensbescherming (FG). Alle toezichthouders zijn onafhankelijk in hun oordeelsvorming en beschikken voor hun taakuitvoering over bijzondere bevoegdheden.

De interne toezichthouders bij Defensie overleggen periodiek met elkaar onder leiding van de Inspecteur-Generaal Veiligheid in het zogenaamde Toezichtberaad. Vanaf eind 2021 is de secretarisrol van dit overleg belegd bij het Ondersteuningsteam Toezicht.

Om de effectiviteit van het toezicht te vergroten, wordt nadrukkelijker en vaker onderling aansluiting gezocht tussen Defensie toezichthouders. Voor de FG's zijn dit met name de Inspectie Militaire Gezondheidszorg (IMG), de Inspectie Veiligheid Defensie (IVD) en de Beveiligingsautoriteit (BA). Binnen het Toezichtberaad is afgesproken dat de samenwerking wordt geïntensiveerd en dat ook de samenwerking met andere interne toezichthouders wordt gezocht. Dit zal vooral zichtbaar zijn in gezamenlijk toezichtbezoeken afleggen en combineren. Vanuit de FG-taken bezien is er veel raakvlak en belang bij het in samenwerking met de BA ontwikkelen van een gezamenlijk onderzoeks- en toetsingskader.

Samenwerking binnen Defensie

In het kader van haar toezichthoudende taak heeft de FG binnen Defensie nauw contact met de Avg-coördinatoren en Wpg privacyfunctionaris als eerste contactpersoon bij de diverse defensieonderdelen. Hierbij geeft de FG ook incidenteel advies, zolang de toezichthoudende rol hiermee niet in het gedrang komt.

Vanuit de BS-/DBE-/Avg-coördinatie is een bijdrage geleverd aan de evaluatie van het Rijksformat DPIA. In de periode oktober- december 2021 zijn voor de Avg-coördinatoren DPIA-trainingen georganiseerd.

De Directie Juridische Zaken (DJZ) is belast met de tweedelijns juridische advisering rond defensiebrede beleidsvorming en juridische advisering omtrent vraagstukken van (politiek) principiële aard, ook ten aanzien van onderwerpen die raken aan de bescherming van persoonsgegevens. Intensivering van de samenwerking met de juridische en operationele lijn is van groot belang. In 2021 heeft de FG herhaaldelijk contact gehad met DJZ, bijvoorbeeld voor de opstelling van een juridisch kader voor het werken in de informatieomgeving, bijdragen aangaande de evaluatie van de Avg en adviezen ten aanzien van internationale gegevensuitwisseling.

Enkele malen is door de FG samengewerkt met de WOB-coördinator van het Ministerie van Defensie, toen in concrete situaties de bescherming van de persoonsgegevens en de openbaarheid van bestuur elkaar raakten.

Aangezien het toezichtdomein voor wat betreft de Avg veel raakvlakken heeft met andere (toezicht)domeinen, zoals integriteit, documentaire informatievoorziening & beveiliging, zijn het afgelopen jaar de samenwerkingsverbanden ook op die vlakken geïntensiveerd. Tevens is, naast de bijdrage van de BA aan het kernteam, betrokken bij het onderzoek naar de verwerkingsactiviteiten bij LIMC, ook aansluiting en ondersteuning gevonden bij de IVD als coördinerend toezichthouder. Dit betrof zowel organisatorische, juridische als facilitaire ondersteuning.

Samenwerking buiten Defensie

Om haar taak goed uit te kunnen voeren, werkt de FG ook samen met personen en instanties buiten de defensieorganisatie. In 2021 is meermaals contact geweest tussen de FG en medewerkers van de Autoriteit Persoonsgegevens (AP).

ADR

De ADR heeft in voorgaande jaren een rijksbreed Avg-onderzoek gedaan waarvan de uitvoering doorliep tot begin 2021. De rode draad rapportage is in mei 2021 aan de CIO rijk aangeboden. Door de ADR is onder meer per departement gekeken naar de invulling van de rechten van betrokkenen en het register van verwerkingsactiviteiten. Om de opvolging van de aanbevelingen die voortkomen uit het rijksbrede Avg-onderzoek te bevorderen voert de ADR *follow-up quickscans* uit.

Voor de KMar is de ADR in 2021 gestart met de uitvoering van de verplichte periodieke Wpg privacy-audit. De uitkomsten daarvan worden in 2022 verwacht.

Internationale samenwerking

Hoewel de Europese wetgeving harmonisatie beoogt, is de bescherming van persoonsgegevens niet in alle landen eenduidig doorgevoerd. Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag daarom alleen als een land voldoende bescherming biedt. Voor doorgifte van gegevens naar een land binnen de Europese Unie (EU) of internationale organisaties gelden andere regels dan voor doorgifte naar een land buiten de EU, zowel in de Avg als in de Wpg.
Dit zorgt ervoor dat Defensie, als internationaal georiënteerde organisatie, voor de juiste naleving van het gegevensbeschermingsrecht in hoge mate afhankelijk is van een goede internationale samenwerking met bondgenoten, partnerlanden en internationale organisaties zoals de NAVO.
In het kader van internationale samenwerking op het gebied van gegevensbescherming zijn er in 2021 (digitale) initiatieven geweest waar een bijdrage aan is geleverd. Dit betreft de voortzetting van de in 2020 opgezette samenwerking vanuit de Military and National Security Data & information protection workshop georganiseerd door het George C. Marshall Centre.

Het RPFG

De voor de FG Avg belangrijkste externe samenwerking vindt plaats in het Rijksplatform van Functionarissen voor de Gegevensbescherming (RPFG). Dit is het overleg van de FG's van de

ministeries en enkele rijksbrede organisaties (ACM, CBS). Het belang van het RPFG is aanzienlijk toegenomen, gezien het toenemende aantal rijksbrede initiatieven en shared service voorzieningen, waarbij ook persoonsgegevens worden verwerkt. Het RPFG wordt steeds meer een gesprekspartner in allerlei rijksbrede trajecten. Daarnaast is binnen het RPFG de invulling afgestemd die is gegeven aan de Privacy Advies Functie Rijk (PAR) bij BZK en het gewijzigde format DPIA.

RPFG voor Wpg en Wjsg

In samenwerking met de FG van de Politie is in 2020 het initiatief genomen een platform of netwerkorganisatie op te richten voor Functionarissen voor Gegevensbescherming, die zijn aangesteld op grond van de Wpg en de Wet justitiële en strafvorderlijke gegevens (Wjsg). In 2021 kon de onderlinge samenwerking weliswaar worden bestendigd, maar is het als platform nog niet voldoende geïnstitutionaliseerd. Het platform is incidenteel en in beperkte samenstelling digitaal bijeengekomen ter bespreking van een aantal concrete onderwerpen.

3 Normering en beoordeling Avg en Wpg

De FG is als onafhankelijke toezichthouder belast met het interne toezicht op de toepassing en naleving van het gegevensbeschermingsrecht, zoals vastgelegd in de Algemene verordening gegevensbescherming (Avg), de Uitvoeringswet Avg (Uavg) en de Wet politiegegevens (Wpg).

De toezichtwerkzaamheden van de FG's richten zich op diverse waarborgen en verplichtingen. Ter uitvoering van de toezichttaak hanteren de FG's verschillende instrumenten en methoden voor het waarnemen en verzamelen van informatie, het afwegen en beoordelen van de verwerkingsactiviteiten en het opstellen en rapporteren van bevindingen, conclusies en aanbevelingen. Daarnaast wordt eveneens aansluiting gezocht bij de focusgebieden, zoals door de AP gehanteerd in het visiedocument 'Dataprotectie in een digitale samenleving: datahandel, digitale overheid en artificiële intelligentie en algoritmes'. Zowel in de bedrijfsvoering als in de operationele taken van Defensie zijn deze ontwikkelingen aan de orde.

Op basis van afspraken in het Toezichtberaad Defensie (het samenwerkingsverband van de interne toezichthouders van Defensie) rapporteren interne toezichthouders in de jaarverslagen waar mogelijk op basis van vaste normeringen. In dit hoofdstuk van het jaarverslag wordt op basis van het toepasselijke normenkader gerapporteerd of de Avg- en Wpg-(onder)beheerders de passende technische en organisatorische maatregelen hebben getroffen om te waarborgen en aan te kunnen aantonen dat de verwerkingen van persoonsgegevens in overeenstemming met de Avg en Wpg worden uitgevoerd. Over de naleving in 2021 wordt aan de hand van de basisnorm en per Avg- of Wpg-(onder)beheerder individueel gerapporteerd. Hierdoor ontstaat een duidelijk en meerjarig beeld van de stand van zaken over de naleving en de aandachts- en verbeterpunten ten aanzien van de Avg en de Wpg bij Defensie.

3.1 De Avg-coördinator en Wpg-privacyfunctionaris

Op grond van artikel 1.3, lid 3, van de Avg Regeling wijst een Avg-(onder)beheerder binnen zijn dienstonderdeel een Avg-coördinator aan. Deze laatste coördineert de uitvoering van de wet en de feitelijke handelingen die daarvoor nodig zijn binnen zijn dienstonderdeel. Op grond van artikel 34 van de Wpg en artikel 1.4 van de Regeling Wpg Defensie dient CKMar als Wpg-beheerder de privacyfunctionarissen aan te wijzen voor de Wpg. De (onder)beheerders doen melding aan de FG van de aanwijzing. De Avg-coördinatoren en privacyfunctionarissen hebben een cruciale rol bij de naleving van de Avg en Wpg in de praktijk bij Defensie. Zij vervullen de belangrijke voorlichtings-, advies- en uitvoeringstaken op het gebied van DPIA's, de melding van datalekken, het registreren van verwerkingsactiviteiten en het behandelen van klachten en rechten van betrokkenen.

In 2021 zijn de volgende normen door de FG ter beoordeling bezien:

a) Is er onder de verantwoordelijkheid van de (onder)beheerder een Avg-coördinator of Wpg-privacyfunctionaris aangewezen?
b) Is deze Avg-coördinator of Wpg-privacyfunctionaris formeel aangemeld bij de FG?
c) Was deze Avg-coördinator of Wpg-privacyfunctionaris bekend gesteld in de organisatie?

d) Heeft deze Avg-coördinator of Wpg-privacyfunctionaris de juiste opleiding/training gekregen voor de functie?
e) Krijgt de Avg-coördinator of Wpg-privacyfunctionaris de benodigde geformaliseerde tijd, middelen en ruimte om de taak naar behoren te kunnen uitvoeren?
f) Is de taak van Avg-coördinator of Wpg-privacyfunctionaris opgenomen in de functieomschrijving van de aangewezen medewerker?

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS (apparaat)	BS DOPS	BS (defensie breed)	DMO	DMO/ JIVC	DOSCO
a				IV			V				
b							V				
c											
d											
e		I/II	II	IV	III	I/II		II			
f				IV		I		I			

Ja/goed	
Onvoldoende	
Nee	
Onbekend/geen info	

Bevindingen

I. In 2021 was bij de KL één halve VTE Avg-coördinator aangesteld en het Avg-onderbeheerderschap belegd bij de brigades. In 2022 zal de Avg-coördinator functie als een volledige VTE worden ingevuld. In 2021 was daarnaast slechts één VTE Avg-(brigade)coördinator aangesteld. Ook bij de brigades komt in 2022 versterking van de Avg-capaciteit. De Avg coördinatiefunctie BS wordt verricht vanuit neventaak op basis van een generieke functiebeschrijving. Halverwege 2021 is de Avg capaciteit bij de BS versterkt.

II. Een aantal defensieonderdelen heeft de afgelopen jaren aandacht besteed aan (her)inrichting van de Avg-coördinatorfunctie. Binnen de BS/DBE zal in 2022 invulling worden gegeven aan de functie van een Chief Privacy Officer (CPO). De benodigde vaste capaciteit of capaciteitsuitbreiding is voor een deel (nog) niet ingevuld en voor een deel slechts tijdelijk. Van belang is de structurele borging van de functies en het verder opbouwen en uitbouwen van de kwaliteit. De privacy-ontwikkelingen vragen immers om op privacy-gebied vaardige Avg-coördinatoren en een goed opgeleid en geëquipeerd onderling netwerk van functies, die multidisciplinair inzetbaar zijn om aan hun taak te kunnen voldoen. Daarnaast is de intensivering van de samenwerking met de juridische en operationele lijn van groot belang.

III. Bij de KMar zijn twee vaste arbeidsplaatsen bij het Cluster Juridische Zaken bestemd voor de Wpg privacyfunctionaris. Heel 2021 was slechts één privacyfunctionaris aangesteld. De privacyfunctionaris KMar is tot het tweede kwartaal 2021 ondersteund door een tijdelijke Wpg-coördinator. De tweede privacyfunctionaris is in februari 2022 aangesteld.

IV. De functie Avg-coördinator KMar was in 2021 aangesteld op een tijdelijke arbeidsplaats van twee jaar die afloopt per juni 2022. De functie was vanaf oktober 2021 vacant en is in het eerste kwartaal 2022 weer gevuld en zal naar verwachting omgezet worden naar een vaste arbeidsplaats. Een aanmerkelijk deel van de capaciteit van de Avg-coördinator KMar was in 2021 nodig voor werkzaamheden voor het programma Future Borders. Vanaf oktober 2021 is een tijdelijke functie aangemaakt om daarvoor extra Avg-capaciteit beschikbaar te stellen.

V. De functie is heel 2021 in neventaak waargenomen. Vulling van de functie door een vakbekwame Avg coördinator is belangrijk voor de continuïteit en kwaliteit van de coördinatie AVG/RGMO en daarmee aansluiting vanuit de operatie. BS DOPS heeft in

februari 2022 een Avg-coördinator aangesteld; tot die datum was de Avg taak belegd bij een interim functionaris.

Aanbeveling

Versterk en professionaliseer de Avg coördinatiefunctie en intensiveer de samenwerking met de juridische en operationele lijn. Investeer in het vergroten van capaciteit en kennisniveau, zowel kwantitatief en kwalitatief waar noodzakelijk.

3.2 Jaarrapportage

Iedere (onder)beheerder behoort jaarlijks, vóór 1 januari, aan de FG te rapporteren over de naleving binnen zijn defensieonderdeel.

Voor het jaar 2021 is het volgende beoordeeld:

a) Heeft de Avg-/Wpg-(onder)beheerder een jaarrapportage aan de FG aangeboden?
b) Is deze rapportage vóór 1 januari aan de FG aangeboden?

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS (apparaat)	BS DOPS	BS (defensiebreed)	DMO/ JIVC	DOSCO
a										
b	I			I	I	I			I	

Ja	
Onvoldoende	
Nee	

Bevindingen

I. Deze (onder)beheerders hebben vóór 31 december 2021 om uitstel verzocht en hebben hiervoor toestemming gekregen en voldaan aan de voorwaarde om uiterlijk 15 februari 2022 de jaarrapportage in te dienen.

3.3 DPIA/Gegevensbescherming Effectbeoordeling

Op grond van artikel 35 Avg en artikel 4c Wpg dient voorafgaand aan de verwerking een beoordeling te worden uitgevoerd van de effecten van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens, wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen.

In artikel 3 van de Regeling Avg Defensie en artikel 3 van de Regeling Wpg Defensie is voorgeschreven dat de DPIA dient te worden uitgevoerd door de proceseigenaar als het om ‘een bepaald uitvoerend proces of ICT-systeem gaat’ en ‘door de betrokken beleidsdirectie voor zover het om een DPIA op wetgeving of beleid gaat’. De Avg-coördinator vervult hierin een adviesrol. Als het noodzakelijk is kan hierbij aanvullende consultatie van de FG plaatsvinden. Na het doorlopen van de DPIA wordt het eindadvies (appreciatie) ingewonnen van de FG. Daarbij moet worden bepaald of er dusdanig hoge restrisico’s zijn dat de verwerking middels de procedure van voorafgaande raadpleging dient te worden voorgelegd aan de Autoriteit persoonsgegevens. De proceseigenaar stelt uiteindelijk de definitieve DPIA vast. De DPIA moet vervolgens worden bijgevoegd in het register van verwerkingsactiviteiten.

Binnen de rijksoverheid wordt gewerkt met een vastgesteld model DPIA. Dit model is in 2021 geactualiseerd. Op grond van de Wpg geldt ook de verplichting tot het uitvoeren van DPIA's; hiervoor moet een aangepaste versie van het rijksmodel worden gehanteerd.

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 de risico's te verkleinen. Als er ondanks de voorgenomen maatregelen onvoldoende zekerheid kan worden geboden dat de verwerking in overeenstemming met de Avg of de Wpg kan worden uitgevoerd, dan kan de verwerking niet aanvangen (of worden voortgezet). In uitzonderlijke gevallen dient te worden overwogen het traject van voorafgaande raadpleging te doorlopen bij de externe toezichthouder: de Autoriteit Persoonsgegevens.

Het doorlopen van een DPIA-proces heeft het karakter van een risico-inventarisatie. Een positieve beoordeling door de FG biedt de garantie dat de DPIA van een bepaalde verwerking beantwoordt aan de wettelijke vereisten uit de Avg of de Wpg. Een DPIA moet periodiek worden herhaald. Ook moet het worden herzien als de verwerking in aanmerkelijke mate wijzigt.

De appreciatie van de FG is doorslaggevend voor de vraag of de DPIA kan worden vastgesteld.

De (definitieve) DPIA dient voorafgaand aan de vaststelling en vóór aanvang van nieuwe verwerkingsactiviteiten, te zijn voorgelegd aan de FG. In 2021 zijn in totaal 22 DPIA's Avg aan de FG voorgelegd ter appreciatie. In 2021 werden in totaal 8 KMar DPIA's Wpg ter consultatie voorgelegd aan de FG.

Er is een sterke toename zichtbaar in het aantal uit te voeren DPIA's en ook de complexiteit neemt toe. Het verplichtende karakter van de DPIA 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 als proceseigenaar of verantwoordelijke beleidsdirectie.

In 2021 is de naleving van de DPIA-verplichting op de volgende normen door de FG ter beoordeling bezien:

a) Worden de wettelijke voorvragen juist doorlopen en wordt er een juiste interpretatie gegeven aan de DPIA-verplichting?
b) Is er een goed overzicht van DPIA's die moeten worden uitgevoerd (inclusief prioritering)?
c) Is de werkvoorraad in verhouding tot de capaciteit (kwantitatief en kwalitatief) van de DPIA-teams
d) Wordt het rijksformat juist gebruikt en volledig ingevuld:
   - Is het proces voldoende beschreven?
   - Zijn wettelijke grondslagen en het juridisch kader voldoende uitgewerkt?
   - Zijn risico's voldoende in kaart gebracht?
   - Zijn er afdoende mitigerende maatregelen genomen of bewuste restrisico's geaccepteerd door procesverantwoordelijke?
   - Is er sprake van formele vaststelling van de definitieve DPIA door de verwerkingsverantwoordelijke?
e) Is de voorgeschreven interne procedure voor aanbieding ter advies van de DPIA juist doorlopen? (consultatie/appreciatie FG en eventueel voorafgaande raadpleging AP)
f) Worden de vastgestelde DPIA's toegevoegd aan het register van verwerkingsactiviteiten?

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS (apparaat)	BS DOPS II	BS (defensie breed)	DMO	DMO/ JIVC	DOSCO
a			I				III				
b											
c		IV	IV					IV	IV	IV	
d	II	II	II	II	II	II		II	II	II	II
e											
f											

Ja/goed	
Onvoldoende	
Nee	
Onbekend/geen info	

Bevindingen

I. Bij CLSK wordt de methode van een QuickScan PIA beproefd om te bepalen of voor een verwerking het DPIA-proces dient te worden doorlopen.
II. Ter verbetering van de kwaliteit van de DPIA's zijn in 2021 masterclasses georganiseerd
III. Op de verwerkingen vanuit BS/DOPS waarop de regeling gegevensverwerking militaire operaties van toepassing is, geldt geen DPIA-verplichting; er is geen informatie over verwerkingen waarop de RGMO niet van toepassing is en waarop dus wel een DPIA-verplichting rust.
IV. CLAS, CLSK, DMO, JIVC, BS (defensiebreed) rapporteren dat de beschikbare capaciteit (kwantitatief en kwalitatief) voor het opstellen van DPIA's een zorgpunt is.

Aanbeveling

Verhoog de kwaliteit van DPIA's en registraties in het register van verwerkingsactiviteiten en investeer in capaciteit en in het vergroten van het kennisniveau op het gegevensbeschermingsdomein.

3.4 Register van verwerkingsactiviteiten (registerplicht)

De verwerkersverantwoordelijke dient in het kader van zijn verantwoordingsplicht een register bij te houden van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden (art.30, lid 1, Avg en art. 31d Wpg). Deze verplichting dient een goed inzicht en overzicht te bieden en vereist een vergaande inventarisatie en uitputtende registratie van alle verwerkingsactiviteiten. Bovendien is doorlopende aandacht voor het onderhouden en actualiseren van het register nodig.
De verwerkingsverantwoordelijke houdt een register bij van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:

- Naam en contactgegevens van de verwerkingsverantwoordelijke en de Avg-coördinatoren en van de FG;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt (inclusief ontvangers in derde landen of internationale organisaties);
- Voor zover van toepassing: doorgiften van persoonsgegevens aan een derde land of een internationale organisatie (artikel 49 lid 1 Avg), de documenten inzake de passende waarborgen;

- Indien mogelijk, de beoogde termijnen waar binnen de verschillende categorieën van gegevens moeten worden gewist;
- Waar mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32 lid 1 Avg.

Voor de verwerkingsactiviteiten die onder de Wpg plaatsvinden geldt deze registerplicht sinds 1 januari 2019. Voor het Avg-verwerkingenregister dat Defensie gebruikt voor het registreren van Wpg-verwerkingen is de benodigde update/systeemrelease eind 2020 beschikbaar gekomen.
De FG heeft over 2021 bezien of de daadwerkelijk geregistreerde verwerkingen in register van verwerkingsactiviteiten valide, volledig en 'up-to-date' zijn.

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS	BS DOPS	BS (defensie breed)	DMO	DMO/ JIVC	DOSCO
		I	I	I	II		III			I	I

Ja	
Onvoldoende	
Nee	
Onbekend/geen info	

Bevindingen

I. Bij de meeste defensieonderdelen is de inventarisatie en registratie van de verwerkingsactiviteiten nog niet op orde. Vaak gaat het om het niet consequent benoemen van de juiste verwerkingsgrondslag. Tevens staan veel gemelde verwerkingsactiviteiten nog 'in bewerking' en/of zijn ze nog niet gepubliceerd. De mogelijke oorzaak is dat de betreffende verwerkingsactiviteiten nog niet op het juiste detail- of abstractieniveau in overzichtelijke structuren of categorieën met vergelijkbare processen of verwerkingen konden worden ingedeeld. Alle verwerkingen van persoonsgegevens dienen volledig gedocumenteerd te zijn (voor zover relevant inclusief de DPIA en de verwerkingenovereenkomst en op het juiste abstractieniveau). In 2022 is beoogd om defensiebreed een structurerings-, kwaliteits- en actualiseringslag door te voeren in het register. Deze kwaliteitsslag is reeds in 2021 door de defensieonderdelen over de gehele linie ingezet.

II. De KMar is per 1 januari 2019 gestart met inventariseren en registreren van de Wpg-verwerkingen, op grond van haar wettelijke verplichting. Aangezien het Avg-verwerkingsregister van Defensie niet op tijd is aangepast en geschikt is gemaakt voor het registreren van Wpg-verwerkingen, is hiervoor een tijdelijke voorziening getroffen. Door capaciteitsgebrek is de noodzakelijke inventarisatie nog niet afgerond en zijn de KMar verwerkingen nog niet (volledig) opgenomen in het register. Dit geldt ook voor de Wpg-verwerkingen. De verwerkingen zijn voor een klein deel opgenomen in het Defensie-verwerkingenregister; de tijdelijke voorziening is niet uitgefaseerd.

III. Verwerkingen vanuit BS/DOPS waarop de Regeling gegevensverwerking militaire operaties van toepassing is worden opgenomen in een apart register van verwerkingsactiviteiten; er is geen informatie over verwerkingen waarop de RGMO niet van toepassing is.

Aanbeveling

Completeer en documenteer het Defensie verwerkingenregister (inclusief DPIA's en verwerkersovereenkomsten).

3.5 Verwerkersovereenkomsten

Er is mogelijk sprake van een 'verwerkersrelatie' wanneer het Ministerie van Defensie als verwerkingsverantwoordelijke (of een van de defensieonderdelen die zijn aangewezen als Avg- of Wpg-(onder)beheerder) een andere overheidsinstantie of -dienst, een natuurlijke persoon of een rechtspersoon wil inschakelen om ten behoeve van Defensie persoonsgegevens te laten verwerken.

Artikel 28 Avg en artikel 6c Wpg bepalen dat, wanneer door een verwerkingsverantwoordelijke een (technisch) verwerker wordt ingeschakeld, hiervoor uitsluitend een verwerker mag worden ingeschakeld die afdoende garanties met betrekking tot de juiste toepassing van technische en organisatorische maatregelen biedt om de naleving van de Avg en de Wpg te kunnen waarborgen. Een en ander dient te zijn vastgelegd in een verwerkersovereenkomst (of andere rechtshandeling, bijvoorbeeld een convenant of een verwerkersafspraak).

Op grond van artikel 1.4 Regeling Avg Defensie en artikel 1.5 van de Regeling Wpg Defensie mogen Avg- en Wpg-(onder)beheerders een dergelijke verwerkersovereenkomst sluiten.

Let wel: dit gaat uitsluitend om situaties waarbij een verwerker wordt ingeschakeld om persoonsgegevens in het belang van het organisatieproces van Defensie, in opdracht- en met strikte instructies van Defensie te gaan verwerken. Een verwerker mag op zijn beurt zonder toestemming van Defensie ook geen andere verwerker inschakelen (een 'sub-verwerker'). De verwerker bepaalt niet zelf het doel en de middelen van de verwerking. Als een andere overheidsdienst of ander (rechts)persoon de persoonsgegevens gaat verwerken ten behoeve van het eigen organisatieproces en op basis van zelf bepaalde doelen en middelen, dan is er geen sprake van een verwerkersrelatie. Dan is er sprake van individuele verwerkingsverantwoordelijken die onderling persoonsgegevens verstrekken en ontvangen, zonder dat daarbij sprake is van een verwerkersrelatie.

In 2021 is de verplichting tot het sluiten van verwerkersovereenkomsten op de volgende aspecten door de FG ter beoordeling bezien:

a) Wordt tijdig en op juiste wijze beoordeeld en vastgesteld of er sprake is van een verwerkersrelatie?
b) Is er een goed overzicht van verwerkersovereenkomsten die nog afgesloten of geactualiseerd dienen te worden?
c) Voldoen de gesloten verwerkersovereenkomsten of afspraken aan de wettelijke vereisten:
   bevat ten minste afspraken over of verwijzingen naar:
   - Het onderwerp en de duur van de verwerking
   - De aard en het doel van de verwerking
   - Het soort persoonsgegevens en de categorieën van betrokkenen
   - Strikte schriftelijke instructies, onder andere voor wat betreft de doorgifte van persoonsgegevens aan derde landen of internationale organisaties
   - Autorisaties en geheimhoudingsplicht
   - Naleving en borging rechten betrokkenen
   - Naleving en procedureafspraken meldplicht datalekken
   - Het wissen/teruggeven van persoonsgegevens na einde overeenkomst
   - Inschakeling subverwerkers
   - Medewerking aan toezicht activiteiten en audits
d) Worden de verwerkersovereenkomsten toegevoegd aan het register van verwerkingsactiviteiten?

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS (apparaat)	BS DOPS	BS (defensie breed)	DMO	DMO/ JIVC	DOSCO
a	I	I	I	I	I	I		I	I	I	I
b											
c	II	II	II	II	II	II			II	II	II
d											

Ja/goed	
Onvoldoende	
Nee	
Onbekend/geen info	
Niet van toepassing	

Bevindingen

I. Er is behoefte aan een eenduidig beleid en overzicht voor het beoordelen en wettelijk juist interpreteren van de relatie tussen Defensie en de partijen waarmee wordt samengewerkt in het licht van de Avg en de Wpg. Het is van groot belang dat gegevensbescherming prominent aan de voorkant van het inkoopproces (inclusief beveiliging en ABDO) wordt meegenomen. Bovendien wordt het onderscheid tussen samenwerkingsrelaties vanuit ieders individuele verwerkingsverantwoordelijkheid, vanuit een gezamenlijke verwerkingsverantwoordelijkheid of op basis van verwerkersrelatie en –overeenkomst, niet in alle gevallen juist gemaakt. Hierdoor worden mogelijk verwerkersovereenkomsten afgesloten in situaties waarin dit niet noodzakelijk is en wordt de verwerkingsverantwoordelijkheid niet belegd bij de juiste partij. Ook voor wat betreft dit onderdeel is in 2021 door de defensieonderdelen over de gehele linie een kwaliteitsslag ingezet.

II. Over het verslagjaar 2021 zijn onvoldoende gegevens beschikbaar.

Aanbeveling

Meer aandacht voor de beveiliging van persoonsgegevens bij de uitwisseling ervan met externe partijen en investeer in het verhogen van de bewustwording (inkoopketen & behoeftestelling).

3.6 Rechten van betrokkene

De Avg kent aan betrokkenen privacyrechten toe. Daartoe is in de aanloop van de inwerkingtreding van de Avg een ‘proces rechten betrokkenen’ ingericht. Een vergelijkbare regeling is ook in de Wpg opgenomen. Hierop gelden echter wel specifieke uitzonderingen die het recht van de betrokkene kunnen beperken als dat nodig is. Bijvoorbeeld wanneer het in het belang van de openbare orde en veiligheid is, of om belemmering in de politietaak of strafrechtelijke onderzoeken te voorkomen.

Externe verzoeken van betrokkenen worden via de internetsite www.defensie.nl naar de juiste behandelaar geleid, zodat verzoeken tijdig en zorgvuldig worden behandeld. Voor medewerkers in werkelijke dienst geldt een vergelijkbaar proces via de intranetpagina privacy en beveiliging.

Recht	Aantal
Recht op informatie	4360
Recht op overdraagbaarheid gegevens (dataportabiliteit)	52
Recht op gegevenswissing (vergetelheid)	50
Recht op beperking verwerking	1
Recht op rectificatie	1
Overige/combinatie	18
Totaal	4482

Tabel 1 Rechten betrokkenen, extern ingediend, 2021 (tot eind december)

De meeste betrokkenen doen een beroep op het recht op informatie uit personeelsdossiers, als onderdeel van stamboomonderzoek. In 2022 zullen de aanvragen over persoonsgegevens van overledenen waar de Avg niet op van toepassing is, apart zichtbaar worden. Door een verhoogde aanvraag en minder capaciteit (onder andere door coronamaatregelen) bij DMO/JIVC/Informatiebeheer zijn de wettelijke behandeltermijnen begin 2021 niet gehaald. In 2021 is deze achterstand geheel ingelopen en werden verzoeken binnen de wettelijke termijn afgehandeld.

Aanvullend werden in 2021 een 61-tal inzageverzoeken Wpg bij de KMar gedaan.

Betrokkenen kunnen hun rechten alleen doen gelden op hun eigen persoonsgegevens. En dus niet op persoonsgegevens van anderen. Dit geldt ook bij WOB-verzoeken. Voor het indienen van een verzoek om inzage of andere privacyrechten is het 'proces rechten betrokkenen' ingericht en te doorlopen.

In het jaar 2021 is ter beperking van de werklast een specificatie aangebracht bij personeelsdossiers (volledig personeelsdossier en overzicht staat van dienst) en medische dossiers. Gedurende de coronacrisis is een significante stijging van het aantal verzoeken waargenomen. Naast bovengenoemde gegevens moet ook vermeld worden dat ondanks het feit dat verzoeken ten aanzien van privacyrechten via het centrale proces dienen te lopen, er ook talrijke verzoeken binnenkomen bij de Avg-coördinatoren van de defensieonderdelen.

Avg klachten/vragen/signalen

Enkele van de vele externe verzoeken hebben geleid tot vragen, veroorzaakt door een vertraagde afhandeling of onduidelijke vraagstelling. Deze vragen zijn afgehandeld, op enkele casussen na. De FG behandelt zelf geen klachten. Wel ziet zij toe op de afhandeling van Avg-/Wpg-klachten door de beheerders. Soms komen er toch klachten bij de FG binnen. Deze worden dan aan de verantwoordelijke beheerder doorgezonden. In 2021 zijn enkele klachten door de FG ontvangen en in samenspraak met de Juridische Dienstverlening (JDV) en de desbetreffende Avg-coördinator afgehandeld. Opvallend is daarin de toename aan gecombineerde Avg-/WOB-verzoeken, mede gerelateerd aan het LIMC-onderzoek.

Privacyverklaring

De privacyverklaring staat zowel op het internet als op het intranet van Defensie, en op andere websites waar persoonsgegevens met Defensie als uitvoeringsverantwoordelijke worden verwerkt, zoals www.rijksoverheid.nl, www.defensie.nl en www.werkenbijdefensie.nl. In deze privacyverklaring is beknopt, transparant en in duidelijke en eenvoudige taal beschreven welke gegevens worden verwerkt en op welke wijze de betrokkenen hun rechten kunnen uitoefenen. In de privacyverklaring wordt specifieke aandacht besteed aan de toepassing van de Wpg op de verwerking van persoonsgegevens bij de KMar.

Overig; meldingen vrijgave account

In geval van overlijden van een medewerker of een ander zwaarwegend belang, zoals bij langdurige ziekte van een medewerker, kan het voorkomen dat het noodzakelijk is om met ondersteuning van Joint Informatie Voorziening Commando (JIVC) toegang te verschaffen tot het digitale account van betrokkene. Hiervoor moet dan door de betreffende Beveiligingscoördinator (BC) toestemming worden verleend. De daadwerkelijke vrijgave vindt vertrouwelijk plaats met gebruikmaking van een tweemansconcept. Van een dergelijke toestemming wordt melding gemaakt bij de FG. In 2021 zijn er vijf van dergelijke meldingen door de FG ontvangen.

3.7 Meldplicht Datalekken/inbreuk op de beveiliging

Datalekken, zoals beschreven in de (herziene) SG aanwijzing 005, worden gemeld in het Melding Voorvallen-systeem (MVV-systeem). De Avg-coördinator of privacyfunctionaris beoordeelt het datalek conform de procedure en consulteert de FG. De tooling die wordt gebruikt voor het MVV loopt echter nog niet synchroon met de te melden Avg-voorvallen/-datalekken. Veelal worden deze in het MVV-systeem gemeld als een 'beveiligingsincident' of 'integriteitskwestie' (* bijzondere gebeurtenis), waardoor de wettelijke termijn (binnen 72 uur) om een datalek te melden bij de AP vaak niet wordt gehaald. Het verdient aanbeveling de MVV tooling hierop aan te passen.

De meldplicht voor datalekken dateert uit 2016 en is in versoepelde vorm opgenomen in de Avg en in de Wpg (sinds 2019). De term datalek werd in artikel 34a Wbp uitgelegd als 'een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'. 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.' Het beoordelen (ofwel het 'wegen') door de Avg-coördinator of een datalek dient te worden beschouwd als een bij de AP meldingsplichtig datalek is daarom juridisch gecompliceerd.

In 2021 zijn door Defensie in totaal 16 datalekken in het kader van de Avg en één datalek in het kader van de Wpg gemeld bij de AP. Dit is redelijk constant in de afgelopen jaren. Voor wat betreft de 'interne' datalekken (de niet bij de AP meldingsplichtige datalekken) zien we echter een toename. Ook deze 'interne' datalekken worden door de Avg-coördinator opgenomen in een datalekregister. In het MVV-systeem worden ook voorvallen gemeld, die aan de Avg raken. De Avg is in het MVV-systeem dan ook een bijzondere categorie, die door de melder expliciet aangevinkt kan worden. De FG ontvangt een afschrift van de zodanig gekwalificeerde meldingen. Deze meldingen worden door de FG aangemerkt als een signaal. Zij kunnen (mede) als basis dienen voor nader toezicht. Dan dient het wel te gaan om een structurele misstand en niet om een op zichzelf staand incident.

In 2021 zijn 154 van dergelijke meldingen door de FG ontvangen. In geen van de gevallen heeft de melding geleid tot het instellen van nader toezicht. Veel meldingen werden gedaan na telefoontjes vanuit het buitenland, phishing mails, openstaande SharePoint/DWRD-omgeving of het hacken van een Facebook-account.

	2021	2020	2019	2018	2017	2016	2015	2014
Avg-gerelateerde MVV-meldingen	154	156	95	75	51	49	37	23
Bij AP (extern) Avg gemelde datalekken	16	15	14	16	18	17	0	0
Wpg-gerelateerde MVV-meldingen	1	5	9	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Bij AP (extern) Wpg gemelde datalekken	1	0	1	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Totaal	**172**	**172**	**104**	**90**	**69**	**66**	**37**	**23**

3.8 Audits

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming is met de Avg en de Wpg. Vanuit de wetgeving ligt de nadruk daarom niet alleen op het naleven en de waarborging (compliance), maar geldt er nadrukkelijk ook een verantwoordingsplicht (accountability). Met andere woorden: het gegevensbeschermingsrecht moet niet alleen worden toegepast en nageleefd, de naleving moet ook aantoonbaar zijn.

Naast de toezichthoudersrol van de FG en het externe toezicht door de Autoriteit Persoonsgegevens is het (laten) uitvoeren van audits een belangrijk instrument. Dit kan gaan om interne- of externe IT-audits. De uitvoering van audits is in beginsel optioneel en zonder vaste normering opgenomen in de Avg. De Avg bevat eigenlijk een 'audit recht' dat de verwerkingsverantwoordelijke met name in staat stelt om aan zijn verantwoordingsplicht te kunnen voldoen en om de nakoming van afspraken met verwerkers (neergelegd in verwerkersovereenkomsten) te controleren middels audits (zie artikel 24 en 28 lid 3 h Avg).

In artikel 7 van de Regeling Avg Defensie is opgenomen dat de Audit Dienst Rijk (ADR), al dan niet op verzoek van de FG of een Avg-beheerder, (periodiek) audits kan laten uitvoeren naar de naleving van de Avg.

De Wpg kent in tegenstelling tot de Avg wel een auditverplichting op grond van artikel 33 Wpg. Deze is nader uitgewerkt in het Besluit politiegegevens[2] en de Regeling periodieke audit politiegegevens. Deze verplichting houdt in dat via interne en via externe audits controles dienen te worden uitgevoerd naar opzet, bestaan en werking van de organisatie en de genomen maatregelen en procedures rond de naleving van de Wpg. Deze audits dienen jaarlijks intern plaats te vinden op deelaspecten van de Wpg en eenmaal per vier jaar dient een volledige en onafhankelijke externe audit te worden uitgevoerd door de ADR. Bij tekortkomingen dienen op basis van een verbeterplan maatregelen te worden genomen en volgt binnen één jaar hercontrole.

Voor 2021 is de uitvoering van de Wpg-audits op de volgende aspecten door de FG ter beoordeling bezien:

a) Is de organisatie bekend met de mogelijkheid dan wel de verplichting tot het uitvoeren van audits?
b) Is er voldoende interne en externe (Adr-)capaciteit beschikbaar voor het uitvoeren van audits?
c) Is er een interne of externe Avg-audit uitgevoerd naar de naleving van de Avg of Wpg?
d) Is de periodiek verplichte (jaarlijks) interne Wpg-audit uitgevoerd?

[2] in werking sinds 1 januari 2009 zie Staatscourant 2008 nr. 252, laatstelijk gewijzigd 21 juni 2019, Staatcourant 2019 nr. 31163

e) Is de laatste periodiek verplichte (vierjaarlijkse) externe Wpg-audit uitgevoerd?
f) Is er een plan van aanpak verbetermaatregelen opgesteld en is de verplichte hercontrole uitgevoerd?

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS (apparaat)	BS (defensie breed)	DMO	DMO/ JIVC	DOSCO
a										
b					II					
c	I	I	I	I	II	I	I	I	I	I
d					II					
e					II					
f					II					

Ja/goed	
Onvoldoende	
Nee	
Onbekend/geen info	
Niet van toepassing	

Bevindingen

I. De Avg-beheerders van de defensieonderdelen hebben 2021 geen audits laten uitvoeren. In 2020-2021 heeft de ADR wel een rijksbrede audit uitgevoerd (rechten betrokkenen en inrichting register van verwerkingsactiviteiten). De audit bevestigt het beeld, dat verbetertrajecten zijn opgestart, inrichting privacymanagement en privacygovernance nog in ontwikkeling is en voldoende privacycapaciteit een aandachtspunt blijft. Voor wat betreft procedures rondom de rechten van betrokkenen leverde dit voor Defensie een positief beeld op.

II. De privacyfunctionaris heeft in 2020 intern onderzoek uitgevoerd naar de Wpg-compliance over de periode 2014-2018. In het derde kwartaal van 2020 is het rapport opgeleverd en gedeeld met de ADR. De ADR voerde, mede op basis van deze uitkomsten, in 2021 de wettelijk verplichte externe audit uit.

Bijlage

Toezichtmethodieken FG

De FG is als onafhankelijke toezichthouder belast met het interne toezicht op de toepassing en naleving van het gegevensbeschermingsrecht, zoals voorgeschreven in de Algemene verordening gegevensbescherming (Avg), de Uitvoeringswet Avg (UAvg) en de Wet politiegegevens (Wpg)[3].

De toezichtwerkzaamheden van de FG's richten zich op diverse waarborgen en verplichtingen. Ter uitvoering van de toezichttaak hanteren de FG's verschillende instrumenten en methoden voor het waarnemen en verzamelen van informatie, het afwegen en beoordelen van de verwerkingen en het opstellen van bevindingen, conclusies en aanbevelingen.

Nalevingstoezicht

Het intern toezicht van de FG betreft voornamelijk nalevingstoezicht. Door toezichtbezoeken en documenten op te vragen, ontstaat het beeld en wordt aan de hand van het vigerende normenkader een oordeel gevormd over de naleving. Hierover wordt in een rapport verslag uitgebracht met de belangrijkste bevindingen, conclusies en aanbevelingen. Behalve gepland toezicht worden ad hoc-toezichtbezoeken uitgevoerd naar aanleiding van incidenten, onregelmatigheden of datalekken.

Regulier en gepland

Bij regulier gepland nalevingstoezicht gaan de FG's op toezichtbezoek bij defensieonderdelen, maar ook bij verwerkers en subverwerkers die data van Defensie verwerken. Ook voor gegevensverwerking bij (sub)verwerkers is en blijft Defensie verantwoordelijk. Daarom valt die gegevensverwerking ook onder het nalevingstoezicht van de FG's.

Ad hoc

Advisering en klachtbehandeling, zijn geen wettelijke toezichtstaken van de FG. Het kan echter wel voorkomen dat een klacht of incident aanleiding is om onderzoek te doen en *ad hoc*- een toezichtbezoek uit te voeren. Dit hangt af van de aard van de klacht of het incident en de ernst van de overtreding. Daarnaast kan een datalekmelding, een vraag om advies of goedkeuring voor een bepaald verwerkingsproces of nieuwe werkwijze aanleiding zijn om te bezien in hoeverre toezicht vooraf (heeft men overal aan gedacht en de juiste keuzes gemaakt) plaats zal vinden. Ook kan er aanleiding zijn om achteraf toezicht te houden op hoe het uiteindelijk gelopen is.

Nalevingstoezicht

De FG's voeren systeemgericht toezicht uit door het monitoren van de kwaliteit en de naleving van de verplichting tot het bijhouden door de verwerkingsverantwoordelijke en de beheerders van het 'register van verwerkingsactiviteiten'. Het register geeft overzicht en inzicht in relevante beleidsontwikkelingen en de inzet van nieuwe technologieën en toepassingen waarbij de verwerking van persoonsgegevens een rol speelt.

Een andere vorm van kwaliteitstoezicht komt naar voren bij de uitvoering van DPIA's. Een DPIA wordt verplicht ter appreciatie aan de FG voorgelegd, pas daarna mag verantwoordelijke of de beheerder de DPIA vaststellen en kan de nieuwe verwerking aanvangen.

---

[3] De FG's bij Defensie zijn **niet** belast met het toezicht op de naleving van de Wet op de inlichtingen en veiligheidsdiensten 2017 door de Militaire Inlichtingen en Veiligheidsdienst (MIVD).

De FG's houden ook 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 Autoriteit Persoonsgegevens. Behalve dat een datalek aanleiding kan vormen voor het instellen van een toezichtbezoek, worden mede op advies van de FG en de BA, maatregelen voorgesteld die een herhaling van het datalek in de toekomst moet voorkomen.

De FG's worden periodiek geïnformeerd en betrokken bij de facultatieve of verplichte audits op de naleving van de Avg en de Wpg die de Audit Dienst Rijk uitvoert bij Defensie. De FG's betrekken de uitkomsten van deze audits en de opvolging van de verbeterpunten in hun toezichtactiviteiten.

Register van verwerkingsactiviteiten

Op grond van de wettelijke verantwoordingsverplichting moeten alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens, alvorens met de verwerking wordt aangevangen, worden vastgelegd in een centraal bij te houden register van verwerkingsactiviteiten. Deze registerplicht is in de plaats gekomen van de oude meldingsplicht bij het College Bescherming Persoonsgegevens (het CBP is de voorloper van de AP).

Met dit centrale register wordt inzichtelijk en overzichtelijk weergegeven welke processen en activiteiten er met persoonsgegevens plaatsvinden inclusief de verwerkingsdoelen en wettelijke grondslagen. Ook wordt vastgelegd op welke wijze en hoe lang de gegevens worden bewaard, aan wie ze worden verstrekt en hoe de beveiliging op hoofdlijnen geregeld is.

Hiermee wordt binnen de eigen organisatie duidelijk gedocumenteerd welke gegevensstromen er zijn en kan desgevraagd richting de interne en de externe toezichthouder direct en transparant verantwoording worden afgelegd.

Appreciatie van DPIA's

Op grond van wettelijke verplichtingen dient er voorafgaand aan de verwerking een beoordeling te worden uitgevoerd van de effecten van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens als een verwerking een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (gelet op de aard, de omvang, de context en de doeleinden daarvan). Dit geldt in het bijzonder voor een verwerking waarbij nieuwe technologieën worden gebruikt.

Ook wordt bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien een DPIA geïnitieerd.

De FG houdt toezicht op de uitvoering van de 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 restrisico's. In bijzondere gevallen kan worden besloten om de verwerking via de wettelijke procedure van voorafgaande raadpleging voor te leggen aan de externe toezichthouder; de Autoriteit Persoonsgegevens.

Het doorlopen van een DPIA-proces heeft het karakter van een risico-inventarisatie. Een positieve beoordeling door de FG biedt de garantie dat de DPIA van een bepaalde verwerking beantwoordt aan de wettelijke vereisten uit de Avg of de Wpg. Een DPIA moet periodiek worden herhaald en in elk geval worden herzien als de verwerking in aanmerkelijke mate wijzigt.

De appreciatie van de FG is doorslaggevend voor de vraag of de DPIA kan worden vastgesteld. De Avg- of Wpg-beheerder stelt uiteindelijk de definitieve DPIA vast.