

Onderzoek AVG

Ministerie van Defensie



Auteur: EIFFEL B.V.

Datum: 13 juli 2022

Versie: 1.2

Inhoud

1	Inleiding	6
1.1	Voorwoord	6
1.2	Doel van het rapport	6
1.3	Opzet van het rapport	7
1.4	Aanleiding	10
1.5	Probleemschets	10
2	Management samenvatting	12
2.1	Aanleiding	12
2.2	Probleemschets	12
2.3	Doel van het rapport	13
2.4	Conclusie	14
	2.4.1 Drie hoofdconclusies	14
	2.4.2 Onderzochte activiteiten en beoordeling	16
3	Opdracht	18
3.1	Doelstelling	18
3.2	Onderzoeksvragen	18
3.3	Afbakening en gevraagd resultaat	19
4	Uitkomsten onderzoek	20
4.1	Toelichting mogelijke knelpunten en risicokader	20
	4.1.1 Toelichting mogelijk knelpunt	20
	4.1.2 Toelichting kader voor risicobeoordeling	20
4.2	Conclusie	22
	4.2.1 Grondslag publieke taak en rechtmatigheid	23
	4.2.2 Grondslag gerechtvaardigd belang voor overheidsinstanties	24
4.3	Activiteiten	27
	Activiteit 1: Directie Communicatie monitort, signaleert en duidt mediaberichten	28
	Activiteit 2: Directie Communicatie verwerkt persoonsgegevens van burgers die vragen stellen via sociale media	31
	Activiteit 3: Defensie Cyber Commando wil een AI ontwikkelen om sociale structuren in kaart te brengen	33
	Activiteit 4: Defensie Cyber Commando zet cyberreservisten in	35

Activiteit 5A: De Genie levert militaire bijstand aan civiele autoriteiten	36
Activiteit 5B: Om Advanced Search Teams voor te bereiden ten behoeve van de algemene gereedstelling wordt gebruikgemaakt van realistische oefenscenario's	39
Activiteit 6: Land Information Manoeuvre Centre wil aan de hand van data science technieken (toekomstig) handelingsperspectief ontwikkelen	42
Activiteit 7: Commando Luchstrijdkrachten wil door middel van simpele zoekopdrachten dreigingen onderzoeken	44
Activiteit 8: De Intelligence, Surveillance and Reconnaissance Division wil een scraper gebruiken om ontwikkelingen te duiden ter ondersteuning van de besluitvorming	47
Activiteit 9A: Het Korps Mariniers van het Commando Zeestrijdkrachten heeft de wens om met een geïntegreerd mobiel interceptieplatform signalen, afkomstig van de mobiele apparaten van de eigen mariniers, te verzamelen en te verwerken.	50
Activiteit 9B: Het Korps Mariniers van het Commando Zeestrijdkrachten heeft de wens om met een geïntegreerd mobiel interceptieplatform signalen, afkomstig van de mobiele apparaten van potentiële vijanden, te verzamelen en te verwerken	53
Activiteit 10A: Het Commando Zeestrijdkrachten voert digitale verkenningen uit door Defensie-gerelateerde onderwerpen of hashtags op het internet te onderzoeken.	56
Activiteit 10B: Het Commando Zeestrijdkrachten slaat mogelijke relevante openbare nieuwsberichten op haar SharePoint.	58
Activiteit 11: De Surface and Assault Training Group van het Commando Zeestrijdkrachten stelt strandverkenningsrapporten op.	60
Activiteit 12: Defensie Materieel Organisatie koopt en verkoopt defensiematerieel	61
Activiteit 13: Joint Informatievoorziening Commando ontwikkelt systemen voor Defensieonderdelen	63
Activiteit 14A: Defensie Cyber Security Centrum beveiligt het interne IT-systeem van Defensie door middel van logging en monitoring	65
Activiteit 14B: <vertrouwelijke bijlage>	68
Activiteit 15: <vertrouwelijke bijlage>	69
Activiteit 16: <vertrouwelijke bijlage>	70
Activiteit 17: <vertrouwelijke bijlage>	71
Activiteit 18: Dienstcentrum Personeelslogistiek houdt zich bezig met de arbeidsmarktcommunicatie	72
Activiteit 19: Dienstcentrum Personeelslogistiek voert arbeidsmarktanalyses uit	74

5 Wettelijk toetsingskader 77

5.1	Inleiding	77
5.2	Opzet	77
5.3	Europees Verdrag voor de Rechten van de Mens	78
5.4	Grondwet	78
5.5	Materieel toepassingsbereik AVG	79
5.6	Territoriaal toepassingsbereik AVG	83
5.7	De beginselen van artikel 5 AVG	83
5.7.1	Rechtmatigheid, behoorlijkheid en transparantie	83
5.7.2	Doelbinding	84
5.7.3	Minimale gegevensverwerking	85
5.7.4	Juistheid	86
5.7.5	Opslagbeperking	86
5.7.6	Integriteit en vertrouwelijkheid	86
5.7.7	Verantwoordingsplicht	87
5.8	De grondslagen van artikel 6 AVG	89
5.8.1	Toestemming betrokkene (sub a)	90
5.8.2	Uitvoering overeenkomst (sub b)	91
5.8.3	Wettelijke verplichting (sub c)	91
5.8.4	Vitaal belang (sub d)	92
5.8.5	Algemeen belang (sub e)	92
5.8.6	Algemene opmerkingen over sub c en sub e	93
5.8.7	Gerechtvaardigd belang (sub f)	94
5.8.8	Gerechtvaardigd belang voor overheidsinstanties	96
5.9	Toepasselijke wet- en regelgeving voor Defensie	97
5.9.1	De Grondwet	98
5.9.2	De Politiewet 2012	99
5.9.3	De Wet veiligheidsregio's	100
5.9.4	Rijkswet geweldgebruik bewakers militaire objecten	100
5.9.5	De Wet ambtenaren Defensie	100
5.9.6	De Kaderwet dienstplicht	101
5.9.7	Algemeen organisatiebesluit Defensie 2021	101
5.9.8	Subtaakbesluiten	101

Bijlage 1 Omschrijving activiteiten 103

Activiteit 1	104
Activiteit 2	115
Activiteit 3	125
Activiteit 4	130
Activiteit 5A	135

Activiteit 5B	142
Activiteit 6	154
Activiteit 7	162
Activiteit 8	174
Activiteit 9A	182
Activiteit 9B	197
Activiteit 10A	210
Activiteit 10B	220
Activiteit 11	230
Activiteit 12	237
Activiteit 13	245
Activiteit 14A	253
Activiteit 14B: <vertrouwelijke bijlage>	265
Activiteit 15: <vertrouwelijke bijlage>	266
Activiteit 16: <vertrouwelijke bijlage>	267
Activiteit 17: <vertrouwelijke bijlage>	268
Activiteit 18	269
Activiteit 19	281
Activiteiten 20 tot en met 22	290
Bijlage 2 Persoonsgegevens per activiteit	300
Bijlage 3 Lijst van afkortingen en begrippen	307
Bijlage 4 Opzet onderzoek	310
Bijlage 5 Programma van Eisen	312

1 Inleiding

1.1 Voorwoord

Als EIFFEL zijn wij trots en verheugd dat de opdracht, een onderzoek bij Defensie uitvoeren in het kader van de Algemene verordening gegevensbescherming (hierna: AVG), aan ons is gegund. Tevens willen wij hierbij alle medewerkers die wij gesproken hebben tijdens ons onderzoek bedanken voor hun constructieve medewerking en openheid tijdens de gesprekken. Tot slot willen wij ook het begeleidingsteam bedanken voor de prettige samenwerking en de ondersteuning bij het ons eigen maken van de organisatie.

1.2 Doel van het rapport

Met dit rapport streven wij als onderzoekers van EIFFEL ernaar om Defensie inzicht te verschaffen in een aantal activiteiten waarbij er mogelijk persoonsgegevens worden verwerkt. Dit inzicht is tweeledig: allereerst geeft het rapport inzicht in de werkwijze per activiteit ten tijde van het onderzoek.¹ Hiermee wordt bedoeld hoe, door wie, met welke systemen/ applicaties de activiteit plaatsvindt en welke persoonsgegevens daarbij mogelijk verwerkt worden. Ten tweede maakt het rapport inzichtelijk of en in hoeverre deze werkwijzen voldoen aan de beginselen van de AVG en de mogelijke knelpunten die hierbij ontstaan.

6

De onderzochte activiteiten zijn op basis van een door Defensie zelf uitgevoerde Quick scan geselecteerd en vertegenwoordigen slechts een klein deel van alle activiteiten bij Defensie. Van elk defensieonderdeel is tenminste één activiteit onderzocht. Het onderzoek vormt hiermee een dwarsdoorsnede én momentopname van activiteiten bij Defensie.

Door met dit rapport op meerdere vlakken inzicht te bieden, kan Defensie bepalen hoe zij zich wil én kan ontwikkelen in de (toekomstige) informatieomgeving om haar taken te kunnen blijven uitvoeren. Het rapport biedt Defensie de kans om intern dialoog te voeren over welke taken zij moet uitvoeren, hoe deze moeten worden uitgevoerd en hoe deze zich verhouden tot de AVG.

¹ Het onderzoek heeft plaatsgevonden van januari 2022 tot en met mei 2022.

1.3 Opzet van het rapport

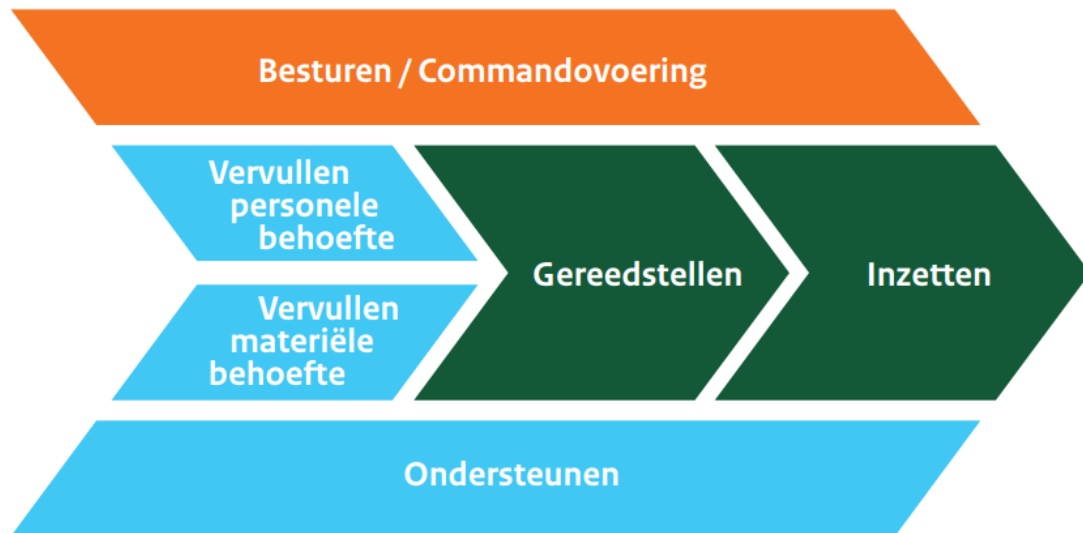
Dit rapport begint met de managementsamenvatting. Vervolgens wordt in het rapport uitgebreider ingegaan op de opdracht. Daarna worden direct de uitkomsten van het onderzoek in de vorm van hoofdconclusies en mogelijke knelpunten omschreven. Tot slot wordt in het laatste hoofdstuk aandacht besteed aan het toegepaste toetsingskader. In *Bijlage 1* is elke activiteit in detail uitgewerkt, waarbij de activiteit aan de AVG beginselen wordt getoetst, de mogelijke knelpunten per activiteit en aanbevelingen zijn opgenomen. In *Bijlage 2* zijn per activiteit de persoonsgegevens die verwerkt kunnen worden opgenomen. Ten slotte staat in *Bijlage 3* de lijst van gebruikte afkortingen, in *Bijlage 4* een toelichting over de opzet van ons onderzoek en in *Bijlage 5* het Programma van Eisen.

Voor een goed begrip van dit rapport is het van belang om enkele begrippen, die regelmatig in dit rapport zullen terugkeren, helder uiteen te zetten:

- De Minister van Defensie: de verwerkingsverantwoordelijke voor de activiteiten waarbij persoonsgegevens worden verwerkt.
- Het Ministerie van Defensie (afgekort: Defensie): het overkoepelende orgaan, bestaande uit: de Koninklijke Marine, de Koninklijke Landmacht, de Koninklijke Luchtmacht, de Koninklijke Marechaussee, het Defensie Ondersteuningscommando, de Defensie Materieel Organisatie, en de Bestuursstaf. Het Ministerie van Defensie draagt zorg voor het goed functioneren van de krijgsmacht en de daarbij behorende beleids-, beheers- en bestuurstaken en verantwoordelijkheden.
- De krijgsmacht: de militair georganiseerde operationele eenheden van het Ministerie van Defensie, bestaande uit diverse gewapende en ondersteunende eenheden van de Koninklijke Marine, de Koninklijke Landmacht, de Koninklijke Luchtmacht, de Koninklijke Marechaussee. Het Defensie Ondersteuningscommando en de Defensie Materieel Organisatie leveren producten, materieel en diensten aan de krijgsmacht.
- Inzet: het handelen van (onderdelen van) de krijgsmacht voor een wettelijke taak, inzet, operatie of missie.
- Gereedstelling: personele gereedheid, materiële gereedheid en geoefendheid. De mate van gereedheid wordt uitgedrukt in operationele gereedheid (algemeen) en inzet gereedheid (specifiek).
- Wet in materiële zin: een besluit van een daartoe bevoegd orgaan die algemeen verbindende voorschriften bevat en niet noodzakelijk afkomstig hoeft te zijn van regering en Staten-Generaal gezamenlijk.

- Wet in formele zin: een regeling die tot stand gebracht wordt door regering en Staten-Generaal tezamen via de grondwettelijke wetgevingsprocedure.

Daarnaast is het ook van belang om kennis te nemen van de waardeketen van Defensie²:



De waardeketen van Defensie geeft de samenhang van primaire en ondersteunende hoofdprocessen weer bij Defensie. De werking van Defensie op basis van de primaire en ondersteunende hoofdprocessen is als volgt:

- Gereedstellen en inzetten (groen) van operationele eenheden vormen gezamenlijk de primaire hoofdprocessen van Defensie. Gereedstelling is het proces van het formeren van eenheden uit personeel en materieel (inclusief IT) om ze vervolgens te oefenen voor hun taken. Personele gereedheid leidt in combinatie met materiele gereedheid en geoefendheid tot operationeel gereede eenheden en dat is bepalend voor de inzetbaarheid van Defensie.
- Om de randvoorwaarden voor deze primaire processen te creëren, zijn ondersteunende processen (blauw) nodig van ondersteunende eenheden: als eerste het vervullen van de personele behoefte met het werven en initieel opleiden van personeel en het vervullen van de materiële behoefte door de verwerving van materieel, met inbegrip van IT en vastgoed. Vervolgens het tijdens de gereedstelling of de inzet leveren van ondersteuning aan de operationele eenheid. Dat kan zijn in de vorm van aanvullende opleidingen voor personeel, militaire gezondheidszorg, specialistisch hoger onderhoud aan materieel,

² Besturen bij Defensie (BBD), A-SG-002, 9 februari 2021.

onderhoud aan vastgoed en IT- infrastructuur, logistieke en facilitaire ondersteuning en informatie en inlichtingenvoorziening.

- Het hoofdproces besturen (oranje) omvat een zevental taken, wat in de context van Defensie neerkomt op:³
 1. Het bepalen van de gezamenlijke missie (in relatie tot de grondwettelijke taken), waarden en gedragsregels voor de defensieorganisatie.
 2. De taak om actief vooruit te kijken, scenario's te ontwikkelen voor de ontwikkeling van de krijgsmacht en de daarvoor benodigde capaciteiten en dit om te zetten in een visie op de toekomst. De visie dient periodiek te worden bijgesteld, om gelet op (inter)nationale ontwikkelingen tijdig de benodigde besluiten over en voor Defensie voor te bereiden. Het is aan de regering om hier besluiten over te nemen en de daarvoor benodigde financiële middelen beschikbaar te stellen. Vervolgens kunnen integraal afgestemde en uitvoerbare beleidsdoelstellingen, de bijbehorende plannen en de begroting worden opgesteld.
 3. De taak om te organiseren, zowel de bestuurlijke als de uitvoerende processen en de uitvoering van projecten; alles wat nodig is om de doelstellingen te realiseren. Bij doelstellingen gaat het om de prestaties (output) en de beoogde effecten (outcome). Daarbij worden Key Performance Indicators (KPI's) gedefinieerd, doelwaarden aan de hand waarvan de mate van doelbereiking kan worden gevolgd.
 4. De taak van leidinggeven, dat wil zeggen het faciliteren en ondersteunen van medewerkers met duidelijke taken, verantwoordelijkheden en bevoegdheden (TVB'n), doelstellingen, de benodigde middelen, opleidingen en coaching zodat zij zich door hun werk kunnen ontwikkelen en zo zelfstandig mogelijk de gestelde taken en doelen kunnen realiseren.
 5. De taak van coördineren, zowel verticaal (hiërarchisch) met opdrachten en de toewijzing van middelen (personeel, financieel, materieel) als het faciliteren van horizontale zelf-coördinatie op operationeel niveau tussen de uitvoerende organisatie-eenheden. Hierbij hoort ook het proactief faciliteren van bottom-up innovatie en initiatieven bij de uitvoerende organisatie-eenheden voor de vernieuwing van Defensie.
 6. De taak van monitoring en regie door tussentijdse effectmetingen of beleidsdoelen/taken/opdrachten gerealiseerd worden en aan wet- en regelgeving wordt voldaan. Waar nodig proactief bijsturen, prioriteiten stellen of opdrachten en beleidsdoelen bijstellen. Onafhankelijke interne

³ Besturen bij Defensie (BBD), A-SG-002, 9 februari 2021, paragraaf 1.2.

en externe toezichthouders spelen hierbij ook een belangrijke rol met hun bevindingen en adviezen.

7. Het afleggen van verantwoording over de realisatie van gestelde doelen/opdrachten, over goed rentmeesterschap over toevertrouwde mensen en middelen en of toegekende bevoegdheden op integere wijze zijn toegepast. Verantwoording afleggen geldt intern Defensie maar ook door de bewindspersonen aan het parlement.

1.4 Aanleiding

De Functionaris Gegevensbescherming AVG Defensie heeft in de periode november 2020 tot maart 2021 een onderzoek uitgevoerd bij het Land Information Manoeuvre Centre (hierna: LIMC) naar de naleving van de AVG bij het verwerken van persoonsgegevens. Naar aanleiding van de bevindingen en aanbevelingen uit het 'Onderzoeksrapport LIMC'⁴ en in de antwoorden op Kamervragen⁵ heeft de Minister van Defensie toegezegd externe capaciteit in te zetten om bij een aantal andere onderdelen/eenheden te onderzoeken en te beoordelen in hoeverre de AVG daar wordt nageleefd bij het verwerken van persoonsgegevens.

1.5 Probleemschets

10

De krijgsmacht heeft drie hoofdtaken die voortkomen uit de Grondwet, namelijk het beschermen van het eigen grondgebied en het grondgebied van bondgenoten, het bevorderen van de (internationale) rechtsorde en stabiliteit en het leveren van bijstand bij rampen en crises. Binnen deze hoofdtaken kan de krijgsmacht in (inter)nationaal verband worden ingezet met inachtneming van (inter)nationale wet- en regelgeving. Het moment waarop, de grondslag waarbinnen activiteiten worden uitgevoerd (oefenen en trainen of inzet), de plaats van de activiteiten (binnen- of buitenland) en de omstandigheden (vredestijd of oorlog) zijn mede bepalend voor wat volgens de juridische kaders wel en niet mag. Bij militaire inzet kan de persoonlijke levenssfeer van burgers (en eigen of vijandige militairen) behalve door fysiek geweld, namelijk ook op andere manieren in het geding komen. Bijvoorbeeld door in een crisis- of oorlogssituatie persoonsgegevens te gaan verwerken voor bepaalde (militaire) doeleinden/context. Defensie geeft aan dat het een probleem is dat er bij uitvoerende eenheden onvoldoende inzicht is in de mogelijkheden en grenzen van juridische kaders op dit vlak en nog onvoldoende is geïdentificeerd wanneer en hoe de juridische kaders de taakuitvoering beperken.

⁴ Zie Kamerbrief 7 mei 2021 (Kenmerk 2021D16726#327-182).

⁵ Zie Antwoorden op Kamervragen 9 april 2021 (Kenmerk 2021D12460 #3218542).

Voor een volledige beschrijving van de probleemschets wordt verwezen naar *Bijlage 5*.

Verder is in het Programma van Eisen bij de scope/ reikwijdte opgenomen: *“Van belang is dat bij de inventarisatie van informatie-activiteiten duidelijk onderscheid gemaakt wordt tussen verwerking in het kader van een van de (hoofd)taken van de krijgsmacht en verwerking in het kader van de bedrijfsvoering”*. Gedurende het onderzoek is deze vraag onderdeel gaan uitmaken van de probleemstelling en is verzocht om deze vraag verder aan te scherpen. Daarom wordt er in het onderzoek per activiteit geduid of er een overloop of samenloop is tussen oefenen, gereedstelling en bedrijfsvoering. Een bijkomende vraag was daarbij ook (wanneer van toepassing) per activiteit een onderscheid te maken tussen het verwerken van persoonsgegevens ter uitvoering van een publieke taak en het verwerken van persoonsgegevens in het licht van taken en bevoegdheden met betrekking tot de bedrijfsvoeringstaken.

2 Management samenvatting

2.1 Aanleiding

De Functionaris Gegevensbescherming AVG Defensie heeft in de periode november 2020 tot maart 2021 een onderzoek uitgevoerd bij het Land Information Manoeuvre Centre (hierna: LIMC) naar de naleving van de AVG bij het verwerken van persoonsgegevens. Naar aanleiding van de bevindingen en aanbevelingen uit het 'Onderzoeksrapport LIMC'⁶ en in de antwoorden op Kamervragen⁷ heeft de Minister van Defensie toegezegd externe capaciteit in te zetten om bij een aantal andere onderdelen/eenheden te onderzoeken en te beoordelen in hoeverre de AVG daar wordt nageleefd bij het verwerken van persoonsgegevens.

2.2 Probleemschets

De krijgsmacht heeft drie hoofdtaken die voortkomen uit de Grondwet, namelijk het beschermen van het eigen grondgebied en het grondgebied van bondgenoten, het bevorderen van de (internationale) rechtsorde en stabiliteit en het leveren van bijstand bij rampen en crises. Binnen deze hoofdtaken kan de krijgsmacht in (inter)nationaal verband worden ingezet met inachtneming van (inter)nationale wet- en regelgeving. Het moment waarop, de grondslag waarbinnen activiteiten worden uitgevoerd (oefenen en trainen of inzet), de plaats van de activiteiten (binnen- of buitenland) en de omstandigheden (vredestijd of oorlog) zijn mede bepalend voor wat volgens de juridische kaders wel en niet mag. Bij militaire inzet kan de persoonlijke levenssfeer van burgers (en eigen of vijandige militairen) behalve door fysiek geweld, namelijk ook op andere manieren in het geding komen. Bijvoorbeeld door in een crisis- of oorlogssituatie persoonsgegevens te gaan verwerken voor bepaalde (militaire) doeleinden/context. Defensie geeft aan dat het een probleem is dat er bij uitvoerende eenheden onvoldoende inzicht is in de mogelijkheden en grenzen van juridische kaders op dit vlak en nog onvoldoende is geïdentificeerd wanneer en hoe de juridische kaders de taakuitvoering beperken.

Voor een volledige beschrijving van de probleemschets wordt verwezen naar *Bijlage 5*.

⁶ Zie Kamerbrief 7 mei 2021 (Kenmerk 2021D16726#327-182).

⁷ Zie Antwoorden op Kamervragen 9 april 2021 (Kenmerk 2021D12460 #3218542).

Verder is in het Programma van Eisen bij de scope/ reikwijdte opgenomen: “Van belang is dat bij de inventarisatie van informatie-activiteiten duidelijk onderscheid gemaakt wordt tussen verwerking in het kader van een van de (hoofd)taken van de krijgsmacht en verwerking in het kader van de bedrijfsvoering”. Gedurende het onderzoek is deze vraag onderdeel gaan uitmaken van de probleemstelling en is verzocht om deze vraag verder aan te scherpen. Daarom wordt er in het onderzoek per activiteit geduid of er een overloop of samenloop is tussen oefenen, gereedstelling en bedrijfsvoering. Een bijkomende vraag was daarbij ook (wanneer van toepassing) per activiteit een onderscheid te maken tussen het verwerken van persoonsgegevens ter uitvoering van een publieke taak en het verwerken van persoonsgegevens in het licht van taken en bevoegdheden met betrekking tot de bedrijfsvoeringstaken.

2.3 Doel van het rapport

Met dit rapport streven wij als onderzoekers van EIFFEL ernaar om Defensie inzicht te verschaffen in een aantal activiteiten waarbij er mogelijk persoonsgegevens worden verwerkt. Dit inzicht is tweeledig: allereerst geeft het rapport inzicht in de werkwijze per activiteit ten tijde van het onderzoek.⁸ Hiermee wordt bedoeld hoe, door wie, met welke systemen/ applicaties de activiteit plaatsvindt en welke persoonsgegevens daarbij mogelijk verwerkt worden. Ten tweede maakt het rapport inzichtelijk of en in hoeverre deze werkwijzen voldoen aan de beginselen van de AVG en de mogelijke knelpunten die hierbij ontstaan.

De onderzochte activiteiten zijn op basis van een door Defensie zelf uitgevoerde Quick scan geselecteerd en vertegenwoordigen slechts een klein deel van alle activiteiten bij Defensie. Van elk defensieonderdeel is tenminste één activiteit onderzocht. Het onderzoek vormt hiermee een dwarsdoorsnede én momentopname van activiteiten bij Defensie.

Door met dit rapport op meerdere vlakken inzicht te bieden, kan Defensie bepalen hoe zij zich wil én kan ontwikkelen in de (toekomstige) informatieomgeving om haar taken te kunnen blijven uitvoeren. Het rapport biedt Defensie de kans om intern dialoog te voeren over welke taken zij moet uitvoeren, hoe deze moeten worden uitgevoerd en hoe deze zich verhouden tot de AVG.

⁸ Het onderzoek heeft plaatsgevonden van januari 2022 tot en met mei 2022.

2.4 Conclusie

2.4.1 Drie hoofdconclusies

Hoofdconclusie 1: grondslag publieke taak en rechtmatigheid

Bij een beperkt aantal activiteiten is er wel een publieke taak toegekend aan Defensie, maar ontbreekt de bevoegdheid om bij het uitvoeren van de betreffende taak persoonsgegevens te mogen verwerken. Een inbreuk op de persoonlijke levenssfeer moet altijd zijn vastgelegd in een wet in formele zin. Die ontbreekt in een aantal gevallen voor Defensie. Dit betekent dat er geen grondslag is om persoonsgegevens te verwerken. Als de activiteit op dit moment wel wordt uitgevoerd, inclusief het verwerken van persoonsgegevens, dan vindt het verwerken van persoonsgegevens onrechtmatig plaats en is dit in strijd met de AVG.

Aan de vastlegging van een bevoegdheid tot het inbreken op de persoonlijke levenssfeer zijn voorwaarden verbonden. De bevoegdheid moet zijn vastgelegd in een wet in formele zin en het verwerken van persoonsgegevens moet noodzakelijk zijn om de taak van algemeen belang of openbaar gezag uit te oefenen. Daarnaast moet de wet duidelijk en nauwkeurig zijn en het moet voor een individu voorspelbaar zijn dat zijn persoonsgegevens worden verwerkt.⁹

14

Hoofdconclusie 2: grondslag gerechtvaardigd belang voor overheidsinstanties

Een van de grondslagen uit artikel 6 AVG is het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG). Hierbij geldt dat overheidsinstanties, zoals het Ministerie van Defensie, zich bij het uitoefenen van hun (wettelijke) taken niet mogen beroepen op deze grondslag.¹⁰ Een beroep op het gerechtvaardigd belang door een overheidsinstantie is alleen mogelijk wanneer er sprake is van een verwerking van persoonsgegevens bij een typisch bedrijfsmatige handeling.

Deze hoofdconclusie is gelaagd en kan aan de hand van vier vragen toegelicht worden:

1. Wanneer kan een overheidsinstelling gebruikmaken van de grondslag gerechtvaardigd belang en welke kaders gelden hiervoor?

Een beroep op het gerechtvaardigd belang door een overheidsinstantie is alleen mogelijk wanneer er sprake is van een verwerking van persoonsgegevens bij een typisch bedrijfsmatige handeling. Binnen Defensie (en mogelijk ook binnen de overheid) ontbreken momenteel duidelijke kaders en richtlijnen voor het gebruik van de grondslag gerechtvaardigd belang. Om te voorkomen dat

⁹ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 lid 1 sub d AVG.

¹⁰ Zie artikel 6 lid 1 sub f AVG. De laatste volzin van dit artikel bepaalt: "De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken."

overheidsinstanties, waaronder Defensie, als het ware misbruik kunnen maken van de grondslag gerechtvaardigd belang is het essentieel dat de overheid duidelijke en strikte voorschriften en richtlijnen maakt. Daarbij is ook van belang om de doelbinding van deze verwerkingen nauwgezet te omschrijven en verdere verwerking te limiteren.

2. Wanneer kun je bij een overheidsinstelling spreken van een typisch bedrijfsmatige handeling?

Een voorbeeld van een typisch bedrijfsmatige handeling voor een overheidsinstantie is de toegangsbeveiliging bij overheidsgebouwen.¹¹ Naast het voorbeeld over toegangsbeveiliging wordt er in de literatuur en de rechtspraak geen nadere uitleg gegeven over typisch bedrijfsmatige handelingen¹² van overheidsinstanties. Het is afhankelijk van alle omstandigheden van de precieze handeling of de overheidsinstantie ook daadwerkelijk een succesvol beroep kan doen op het gerechtvaardigd belang.

3. Als er sprake is van mogelijke overlap bij een activiteit op grond van de grondslag publieke taak en gerechtvaardigd belang (typische bedrijfsmatige handeling), kun je de grens tussen deze twee bepalen?

Bij sommige onderzochte activiteiten zou er sprake kunnen zijn van een typisch bedrijfsmatige handeling, maar is er ook een publieke taak die vergelijkbaar is met een bedrijfsmatige handeling. Als hier sprake van is, is niet altijd te bepalen wanneer welke grondslag van toepassing is. Dit is extra lastig omdat er (zoals benoemd onder vraag 1) momenteel binnen Defensie duidelijke kaders en richtlijnen ontbreken voor het gebruik van de grondslag gerechtvaardigd belang voor typische bedrijfsmatige activiteiten.

4. Voldoet de verwerking aan de cumulatieve voorwaarden voor gerechtvaardigd belang én valt de belangenafweging ook in het voordeel van de overheidsinstelling uit?

Als er bij een activiteit sprake is van een typisch bedrijfsmatige handeling, dan moet voor toepassing van de grondslag gerechtvaardigd belang éérst ook de gerechtvaardigd belang toets worden uitgevoerd. Bij deze toets wordt er getoetst aan de drie cumulatieve vereisten¹³ van artikel 6 lid 1 sub f AVG. Tenslotte moet elke verwerking van persoonsgegevens ook voldoen aan de beginselen van artikel 5 AVG.

¹¹ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 AVG.

¹² In zijn algemeenheid kan worden gedacht aan activiteiten met betrekking tot HR, financiën, interne audit, marketing, communicatie, inkoop en beveiliging die typisch bedrijfsmatige handelingen zouden kunnen zijn voor een overheidsinstantie.

¹³ Het belang moet gerechtvaardigd zijn als rechtsbelang (1), de verwerking van persoonsgegevens moet noodzakelijk zijn om dit belang te behartigen (2) en er moet een belangenafweging worden gemaakt tussen de belangen van de verwerkingsverantwoordelijke en de belangen van de betrokkene (3).

Hoofdconclusie 3: de beginselen van artikel 5 AVG

De laatste conclusie is dat bij sommige activiteiten wel een grondslag is conform artikel 6 AVG, maar dat niet altijd aan de beginselen van artikel 5 AVG wordt voldaan. Er wordt bijvoorbeeld niet voldaan aan het beginsel van transparantie en de verantwoordingsplicht.

2.4.2 Onderzochte activiteiten en beoordeling

In het totaal zijn er in dit onderzoek tweeëntwintig (22) activiteiten beoordeeld, waarbij vier (4) activiteiten weer verder zijn onderverdeeld in twee sub-activiteiten, in totaal zijn er dan ook zesentwintig (26) activiteiten beoordeeld. Bij de beoordeelde activiteiten kunnen één of meerdere mogelijke knelpunten worden geconstateerd. Een mogelijk knelpunt bij een activiteit kan een risico inhouden voor Defensie en een onrechtmatige inbreuk op de persoonlijke levenssfeer van betrokkenen. Aan de hand van de mogelijke knelpunten per activiteit kan aan een activiteit een risicoclassificatie worden toegekend. Dit hebben wij gedaan door middel van een stoplichtsysteem:

- Groen: de activiteit voldoet volledig aan de AVG, de eventuele aanbevelingen blokkeren de doorgang van de activiteit niet.
- Oranje: de activiteit voldoet grotendeels aan de AVG, maar er moeten nog aanvullende vervolgstappen worden genomen om volledig aan de AVG te voldoen. Deze vervolgstappen zijn ook op (korte) termijn realiseerbaar. Als de vervolgstappen niet worden uitgevoerd dan wordt er niet volledig voldaan aan de AVG.
- Rood: de activiteit voldoet niet aan de AVG. Er zijn op (korte) termijn geen vervolgstappen realiseerbaar om de activiteit te laten voldoen aan de AVG. De knelpunten blokkeren de doorgang van de activiteit.

Er zijn tweeëntwintig (22) hoofd- activiteiten, waarbij vier (4) activiteiten weer verder zijn onderverdeeld in twee sub- activiteiten en zijn dus in totaal zesentwintig (26) activiteiten beoordeeld tijdens het onderzoek:

- Twaalf (12) activiteiten hebben de kleur groen gekregen. Van deze twaalf (12) activiteiten zijn er zeven (7) activiteiten waarbij de AVG niet van toepassing is of er niet getoetst is aan de AVG omdat de verantwoordelijkheid voor de activiteiten niet bij Defensie ligt (Defensie is geen verwerkingsverantwoordelijke).
- Zeven (7) activiteiten hebben de kleur oranje gekregen.
- Zeven (7) activiteiten hebben de kleur rood gekregen.

In de onderstaande tabel geeft de kleur de ernst van knelpunten per activiteit aan, indien die plaatsvindt.

Activiteit voldoet volledig aan de AVG en vond plaats tijdens het onderzoek, eventuele aanbevelingen blokkeren de doorgang niet	Activiteit met knelpunt(en), maar de betreffende activiteit vindt niet, niet meer of nog niet plaats	Activiteiten met knelpunten die tijdens het onderzoek plaatsvonden. Dit moet voor een aantal activiteiten geverifieerd worden.
3	6	1
4	7	2
11	8	5B
12	9A	10B
13	9B	14A
15	10A	14B
16		17
18		19
20		
21		
22		
5A		

3 Opdracht

In de periode van januari 2022 tot en met april 2022 heeft EIFFEL onderzoek gedaan naar tweeëntwintig (22) activiteiten bij Defensie. In dit onderzoek lag de focus op de toets van deze activiteiten aan de beginselen van de AVG en mogelijke knelpunten die er spelen bij de taakuitoefening van Defensie. Bij de taakuitoefening wordt er een onderscheid gemaakt tussen algemene taken die aan het Ministerie van Defensie zijn opgelegd en taken die specifiek zijn opgelegd aan de krijgsmacht. De algemene taken van het Ministerie van Defensie worden uitgevoerd door de Bestuursstaf, het Defensie Ondersteuningscommando en de Defensie Materieel Organisatie. De taken die zijn opgelegd aan de krijgsmacht worden uitgevoerd door de Koninklijke Marechaussee, de Koninklijke Luchtmacht, de Koninklijke Landmacht en de Koninklijke Marine. In dit onderzoek zal per taak worden bekeken of er sprake is van een verwerking van persoonsgegevens en of de verwerking plaatsvindt ter uitoefening van een publieke taak of in het kader van interne bedrijfsvoering.

3.1 Doelstelling

18

De doelstelling¹⁴ van het onderzoek is tweeledig:

1. Inventariseer verwerkingen met persoonsgegevens bij eenheden/onderdelen van Defensie waarbij op basis van de eerder uitgevoerde QuickScan twijfel bestaat of de beginselen van de AVG in voldoende mate worden nageleefd.
2. Inventariseer, op basis van een selectie uit de eerder uitgevoerde QuickScan, de door de eenheden/onderdelen (gepercipieerde) juridische knelpunten voor de uitvoering van hun taken en doe aanbevelingen voor het oplossen van bestaande knelpunten.

3.2 Onderzoeksvragen

Per doelstelling moeten de volgende onderzoeksvragen worden beantwoord:

1. Subdoelstelling 1:
 - In hoeverre is er bij de onderdelen/eenheden sprake van verwerking van persoonsgegevens waarbij twijfel bestaat of de beginselen inzake de verwerking van persoonsgegevens van de AVG worden nageleefd?
- Specificeer op basis van:
- Rechtmatigheid;

¹⁴ De doelstelling is conform de doelstelling zoals opgenomen in het Programma van Eisen behorende bij referentienummer 19436041.

- Behoorlijkheid en transparantie;
 - Doelbindingsbeginsel;
 - Beginsel van dataminimalisatie;
 - Juistheidsbeginsel;
 - Beginsel van opslagbeperking;
 - Beginsel van integriteit en vertrouwelijkheid;
 - Verantwoordingsplicht.
- Welke aanbevelingen kunnen, in voorkomend geval, worden gedaan voor het naleven van de AVG?
2. Subdoelstelling 2:
- In hoeverre is er bij de onderdelen/eenheden sprake van knelpunten in de taakuitvoering die voortvloeien uit naleven van overige vigerende juridische kaders voor optreden in de informatieomgeving? Specificeer de geconstateerde knelpunten.
 - Welke aanbevelingen kunnen worden gedaan voor oplossen van de (gepercipieerde) knelpunten binnen de vigerende juridische kaders?

3.3 *Afbakening en gevraagd resultaat*

De scope van dit onderzoek is beperkt tot het verwerken van gegevens ten behoeve van de eigen taken van het Ministerie van Defensie en de krijgsmacht. Het verspreiden van informatie naar en beïnvloeden van actoren buiten Defensie in een informatieomgeving zijn buiten scope.

De reikwijdte is beperkt tot het verwerken van gegevens op Nederlands nationaal grondgebied (inbegrepen marineschepen).

Van belang is dat bij de inventarisatie van informatie-activiteiten duidelijk onderscheid gemaakt wordt tussen verwerkingen in het kader van een van de (hoofd)taken van het Ministerie van Defensie en verwerkingen in het kader van de taken van de krijgsmacht. De activiteiten in dit onderzoek vinden plaats in Nederland in vredetijd, waarbij de activiteit kan bijdragen aan de interne bedrijfsvoering enerzijds en gereedstelling en/of inzet anderzijds.

Het gevraagde resultaat is een rapport waarin de onderzoeksvragen worden beantwoord en aanbevelingen voor aanpassingen en verbeteringen zijn opgenomen.

4 Uitkomsten onderzoek

In dit hoofdstuk worden de conclusies van het onderzoek gedeeld: welke (overkoepelende) mogelijke knelpunten zien wij terug bij de verschillende activiteiten. Vervolgens worden de beoordeelde activiteiten kort beschreven met de mogelijke knelpunten en geadresseerd hoe daarmee om kan worden gegaan. Voor een volledige omschrijving van elke activiteit, de toets aan de beginselen van artikel 5 AVG en de bijbehorende mogelijke knelpunten wordt verwezen naar *Bijlage 1* van dit rapport.

4.1 Toelichting mogelijke knelpunten en risicokader

4.1.1 Toelichting mogelijk knelpunt

De mogelijke knelpunten zijn onderverdeeld in drie hoofdthema's: juridische, organisatorische en ethische knelpunten. Een mogelijke knelpunt is juridisch als de activiteit niet of niet concreet genoeg is omschreven in bestaande wet- en regelgeving of doordat verschillende wetten niet met elkaar communiceren en/of niet op elkaar aansluiten. Een mogelijk knelpunt is organisatorisch van aard als bij de uitvoering van een activiteit intern bij Defensie bepaalde zaken niet op orde zijn zoals bijvoorbeeld kennis van de AVG of als het knelpunt ziet op samenwerking of communicatie tussen verschillende afdelingen. Een mogelijk knelpunt is ethisch van aard op het moment dat een activiteit wellicht wel juridisch toegestaan is, maar de vraag is of de activiteit ethisch verantwoord is. Het knelpunt ziet toe op normen en waarden en hoe deze worden uitgelegd en toegepast.

Dat tijdens ons onderzoek iets als mogelijk knelpunt is geïdentificeerd, brengt niet automatisch met zich mee dat Defensie de geadviseerde oplossing voor het mogelijke knelpunt één op één moet overnemen. Het is aan Defensie om een mogelijk knelpunt te wegen, te valideren en te beoordelen of en zo ja welke eventuele vervolgacties moeten worden genomen om het mogelijke knelpunt weg te nemen.

4.1.2 Toelichting kader voor risicobeadoordeling

Bij de beoordeelde activiteiten kunnen één of meerdere mogelijke knelpunten worden geconstateerd. Een mogelijk knelpunt bij een activiteit kan een risico inhouden voor Defensie en een inbreuk op de persoonlijke levenssfeer van betrokkene. Aan de hand van de mogelijke knelpunten per activiteit kan aan

een activiteit een risicoclassificatie worden toegekend. Dit hebben wij gedaan door middel van een stoplichtsysteem:

- Groen: de activiteit voldoet volledig aan de AVG. Hierbij kan het zo zijn dat er nog een aanbeveling is opgenomen om de 'puntjes op de i' te zetten. De aanbevelingen blokkeren de doorgang van de activiteiten niet.
- Oranje: de activiteit voldoet grotendeels aan de AVG, maar er moeten nog aanvullende vervolgstappen worden genomen om volledig aan de AVG te voldoen. Een activiteit kan ook de kleur oranje hebben gekregen als het onduidelijk is of er beroep gedaan kan worden op de grondslag gerechtvaardigd belang of als het onduidelijk is voor welk deel van de activiteit welke grondslag geldt: publieke taak of gerechtvaardigd belang. De aanbevolen vervolgstappen zijn ook op (korte) termijn realiseerbaar. Als de vervolgstappen niet worden uitgevoerd dan wordt er niet volledig voldaan aan de AVG.
- Rood: de activiteit voldoet niet aan de AVG. Er zijn op (korte) termijn geen vervolgstappen realiseerbaar om de activiteit te laten voldoen aan de AVG. De knelpunten blokkeren de doorgang van de activiteiten.

Om tot een risicoweging te komen is beoordeeld in hoeverre wel of niet wordt voldaan aan de beginselen uit artikel 5 AVG, welke soort persoonsgegevens worden verwerkt en type betrokkenen. De weging is zuiver juridisch van aard. De beoordeling van de rechtmatigheid van een activiteit, meer specifiek de grondslag van een activiteit, is slechts marginaal uitgevoerd. Het is een beperkte toetsing waarbij is gekeken naar de taak en de – indien aanwezig – bijbehorende bevoegdheid tot het verwerken van persoonsgegevens. Artikel 10 Gw heeft als uitgangspunt dat een overheidsinstantie zich, bij de uitvoering van haar taken, dient te onthouden van optreden dat een inbreuk maakt op het recht op eerbiediging en de bescherming van de persoonlijke levenssfeer van een betrokkene, tenzij de overheidsinstantie bij de verwerking van persoonsgegevens voldoet aan de voorwaarden die daaromtrent zijn gesteld. In dat licht zijn wij uitgegaan van de noodzaak van een wet in formele zin en hebben wij de activiteit niet inhoudelijk aan de bevoegdheid getoetst.

Bepaalde factoren vormen een risico op de eerbiediging van de persoonlijke levenssfeer van een betrokkene. Bijvoorbeeld (1) het ontbreken van een grondslag, (2) het niet voldoen aan het beginsel van opslagbeperking en/of het beginsel van minimale gegevensverwerking (uit artikel 5 AVG) en (3) het verwerken van bijzondere persoonsgegevens (als bijvangst). Deze risico's kunnen worden ondervangen door bijvoorbeeld (1) toestemming te vragen of een wettelijke grondslag te creëren, (2) bewaartermijnen en protocollen vast te stellen, en (3) waarborgen in te bouwen om te voorkomen dat er bijzondere persoonsgegevens worden verwerkt.

4.2 Conclusie

In deze paragraaf behandelen we de drie conclusies die uit het onderzoek naar voren komen. In het totaal zijn er in dit onderzoek tweeëntwintig (22) activiteiten beoordeeld, waarbij vier (4) activiteiten weer verder zijn onderverdeeld in twee sub activiteiten. In totaal zijn in het rapport zesentwintig (26) activiteiten beschreven. Bij de beoordeelde activiteiten kunnen één of meerdere mogelijke knelpunten worden geconstateerd. Een mogelijk knelpunt bij een activiteit kan een risico inhouden voor Defensie en een inbreuk op de persoonlijke levenssfeer van betrokkene. Aan de hand van de mogelijke knelpunten per activiteit kan aan een activiteit een risicoclassificatie worden toegekend. Dit hebben wij gedaan door middel van een stoplichtsysteem:

- Groen: de activiteit voldoet volledig aan de AVG. Hierbij kan het zo zijn dat er nog een aanbeveling is opgenomen om de 'puntjes op de i' te zetten. De aanbevelingen blokkeren de doorgang van de activiteiten niet.
- Oranje: de activiteit voldoet grotendeels aan de AVG, maar er moeten nog aanvullende vervolgstappen worden genomen om volledig aan de AVG te voldoen. Een activiteit kan ook de kleur oranje hebben gekregen als het onduidelijk is of er beroep gedaan kan worden op de grondslag gerechtvaardigd belang of als het onduidelijk is voor welk deel van de activiteit welke grondslag geldt: publieke taak of gerechtvaardigd belang. De aanbevolen vervolgstappen zijn ook op (korte) termijn realiseerbaar. Als de vervolgstappen niet worden uitgevoerd dan wordt er niet volledig voldaan aan de AVG.
- Rood: de activiteit voldoet niet aan de AVG. Er zijn op (korte) termijn geen vervolgstappen realiseerbaar om de activiteit te laten voldoen aan de AVG. De knelpunten blokkeren de doorgang van de activiteiten.

22

Er zijn tweeëntwintig (22) hoofd- activiteiten waarbij vier (4) activiteiten weer verder zijn onderverdeeld in twee sub- activiteiten, in totaal dus zesentwintig (26) activiteiten die beoordeeld zijn tijdens het onderzoek:

- Twaalf (12) activiteiten hebben de kleur groen gekregen. Van deze twaalf (12) activiteiten zijn er zeven (7) activiteiten waarbij de AVG niet van toepassing is of er niet getoetst is aan de AVG omdat de verantwoordelijkheid voor de activiteiten niet bij Defensie ligt (Defensie is geen verwerkingsverantwoordelijke).
- Zeven (7) activiteiten hebben de kleur oranje gekregen.
- Zeven (7) activiteiten hebben de kleur rood gekregen.

In de onderstaande tabel geeft de kleur de ernst van knelpunten per activiteit aan, indien die plaatsvindt.

Activiteit voldoet volledig aan de AVG en vond plaats tijdens het onderzoek, eventuele aanbevelingen blokkeren de doorgang niet	Activiteit met knelpunt(en), maar de betreffende activiteit vindt niet, niet meer of nog niet plaats	Activiteiten met knelpunten die tijdens het onderzoek plaatsvonden. Dit moet voor een aantal activiteiten geverifieerd worden.
3	6	1
4	7	2
11	8	5B
12	9A	10B
13	9B	14A
15	10A	14B
16		17
18		19
20		
21		
22		
5A		

4.2.1 Grondslag publieke taak en rechtmatigheid

De belangrijkste conclusie van dit onderzoek, is dat bij een beperkt aantal activiteiten wel een publieke taak is toegekend, maar dat er geen bevoegdheid is toegekend om bij het uitvoeren van de betreffende taak persoonsgegevens te mogen verwerken. Dit betekent dat er geen grondslag is om persoonsgegevens te mogen verwerken. Als de activiteit op dit moment wel wordt uitgevoerd, inclusief het verwerken van persoonsgegevens, dan vindt het verwerken van persoonsgegevens onrechtmatig plaats en is dit in strijd met de AVG.

Het recht op eerbiediging van de persoonlijke levenssfeer is een direct werkend recht dat een verplichting inhoudt voor de overheid om zich van optreden te onthouden, tenzij een wet in formele zin daartoe een grondslag biedt. Een nadere omlijning van het begrip 'persoonlijke levenssfeer' moet gezocht worden in de rechtspraak, waarbij jurisprudentie van het EHRM over artikel 8 EVRM een rol speelt.¹⁵

¹⁵ Tekst & Commentaar Privacy- en gegevensbeschermingsrecht, artikel 10 Grondwet.

Dit betekent dat naast elke toegekende taak, ook in een wet in formele zin moet zijn opgenomen welke bevoegdheden er zijn met betrekking zijn tot het verwerken van persoonsgegevens bij het uitvoeren van de desbetreffende taak. Dat er sprake moet zijn van een formeel wettelijke basis blijkt ook uit een uitspraak van de Hoge Raad, waarin is opgenomen dat “(...) De woorden *“behoudens bij of krachtens de wet te stellen beperkingen” in artikel 10 van de Grondwet brengen bovendien mee dat beperkingen op het recht op eerbiediging van de persoonlijke levenssfeer slechts kunnen worden gerechtvaardigd door of krachtens een wet in formele zin (...)*”.¹⁶ De Raad van State volgt deze lijn ook in zijn voorstel inzake de Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid.¹⁷ Een taak die volgt uit een wet in materiële zin, zoals het Algemeen organisatiebesluit Defensie 2021 of een daaronder liggend subtaakbesluit, kan voor Defensie op zichzelf dus nog geen wettelijke basis vormen voor een rechtmatige verwerking van persoonsgegevens. De bevoegdheid voor het verwerken van persoonsgegevens kan alleen worden afgeleid uit een wet in formele zin. Aan de vastlegging van een dergelijke bevoegdheid zijn voorwaarden verbonden. Het verwerken van persoonsgegevens moet noodzakelijk zijn om de taak van algemeen belang of openbaar gezag uit te oefenen. Daarnaast moet de wet moet duidelijk en nauwkeurig zijn en het moet voor een individu voorspelbaar zijn dat zijn persoonsgegevens worden verwerkt.¹⁸ In hoofdstuk 5 van dit rapport wordt hier nader op in gegaan.

4.2.2 Grondslag gerechtvaardigd belang voor overheidsinstanties

Een van de grondslagen uit artikel 6 AVG is het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG). Hierbij geldt dat overheidsinstanties, zoals het Ministerie van Defensie, zich bij het uitoefenen van hun (wettelijke) taken niet mogen beroepen op deze grondslag.¹⁹ Een beroep op het gerechtvaardigd belang door een overheidsinstantie is alleen mogelijk wanneer er sprake is van een verwerking van persoonsgegevens bij een typisch bedrijfsmatige handeling. Wanneer hiervan sprake is wordt hieronder nader toegelicht.

Deze hoofdconclusie is gelaagd en kan aan de hand van vier vragen toegelicht worden:

1. Wanneer kan een overheidsinstelling gebruikmaken van de grondslag gerechtvaardigd belang en welke kaders gelden hiervoor?

¹⁶ Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:288 rechtsoverweging 2.3.2.

¹⁷ Raad van State No. W16.21.0218/II

¹⁸ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 lid 1 sub d AVG.

¹⁹ Zie artikel 6 lid 1 sub f AVG. De laatste volzin van dit artikel bepaalt: “De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken.”

2. Wanneer kun je bij een overheidsinstelling spreken van een typisch bedrijfsmatige handeling?
 3. Als er sprake is van mogelijke overlap bij een activiteit op grond van de grondslag publieke taak en gerechtvaardigd belang kun je de grens tussen deze twee bepalen?
 4. Voldoet de verwerking aan de cumulatieve voorwaarden voor gerechtvaardigd belang én valt de belangenafweging ook in het voordeel van de overheidsinstelling uit?
1. Wanneer kan een overheidsinstelling gebruikmaken van de grondslag gerechtvaardigd belang en welke kaders gelden hiervoor?

Een beroep op het gerechtvaardigd belang door een overheidsinstantie is alleen mogelijk wanneer er sprake is van een verwerking van persoonsgegevens bij een typisch bedrijfsmatige handeling. Binnen Defensie (en mogelijk ook binnen de overheid) ontbreken momenteel duidelijke kaders en richtlijnen voor het gebruik van de grondslag gerechtvaardigd belang. Om te voorkomen dat overheidsinstanties, waaronder Defensie, als het ware misbruik kunnen maken van de grondslag gerechtvaardigd belang is het essentieel dat de overheid duidelijke en strikte voorschriften en richtlijnen maakt. Daarbij is ook van belang om de doelbinding van deze verwerkingen nauwgezet te omschrijven en verdere verwerking te limiteren.

25

2. Wanneer kun je bij een overheidsinstelling spreken van een typisch bedrijfsmatige handeling?

Een voorbeeld van een typisch bedrijfsmatige handeling voor een overheidsinstantie is de toegangsbeveiliging bij overheidsgebouwen.²⁰ Naast het voorbeeld over toegangsbeveiliging wordt er in de literatuur en de rechtspraak geen nadere uitleg gegeven over typisch bedrijfsmatige handelingen van overheidsinstanties. In zijn algemeenheid kan worden gedacht aan activiteiten met betrekking tot HR, financiën, interne audit, marketing, communicatie, inkoop en beveiliging die typisch bedrijfsmatige handelingen zouden kunnen zijn voor een overheidsinstantie. Het is afhankelijk van alle omstandigheden van de precieze handeling of de overheidsinstantie ook daadwerkelijk een succesvol beroep kan doen op het gerechtvaardigd belang.

3. Als er sprake is van mogelijke overlap bij een activiteit op grond van de grondslag publieke taak en gerechtvaardigd belang (typische bedrijfsmatige handeling), kun je de grens tussen deze twee bepalen?

²⁰ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 AVG.

Een overheidsinstantie, zoals het Ministerie van Defensie, mag zich bij het uitoefenen van haar (wettelijke) taken niet beroepen op de grondslag gerechtvaardigd belang.²¹ Alleen bij de verwerking van persoonsgegevens voor een typisch bedrijfsmatige handeling kan een overheidsinstantie mogelijk wel gebruikmaken van de grondslag gerechtvaardigd belang.

Bij sommige onderzochte activiteiten zou er sprake kunnen zijn van een typisch bedrijfsmatige handeling, maar is er ook een publieke taak die vergelijkbaar is met een bedrijfsmatige handeling. Een voorbeeld hiervan is de beveiliging van Defensie gebouwen, terreinen en eigendommen van Defensie. Beveiliging van eigendommen kan voor een overheidsinstelling een typisch bedrijfsmatige handeling zijn, als de beveiliging vergelijkbaar is met de beveiliging van normale bedrijfspanden. Defensie heeft echter ook de bevoegdheid om geweld toe te passen bij een bedreiging van defensie eigendommen. De 'normale' beveiliging kan plaatsvinden op basis van de grondslag gerechtvaardigd belang. Vanaf het moment dat er echter geweld wordt ingezet conform de Rijkswet geweldgebruik bewakers militaire objecten is dit mogelijk geen typisch bedrijfsmatige handeling meer, maar wellicht wel een publieke taak tot geweldgebruik bij bedreiging voor defensie eigendommen.

Een ander voorbeeld is de activiteit van de Directie Communicatie (hierna: DCo). DCo monitort, signaleert en duidt mediaberichten voor communicatiedoeleinden, zodat de top van Defensie, de minister en de staatssecretaris op de hoogte zijn van wat er speelt in de maatschappij rondom Defensie. Om aan deze informatiebehoefte te voldoen verstuurt DCo een nieuwsbrief aan haar stakeholders. Het versturen van een nieuwsbrief kan worden aangemerkt als typisch bedrijfsmatige handeling. Echter is het toevoegen van persoonsgegevens (zoals namen van journalisten of auteurs) mogelijk niet meer als typisch bedrijfsmatig aan te merken. In dit geval ontbreekt er echter ook een publieke taak en bevoegdheid die in formele wet zijn vastgelegd op grond waarvan er persoonsgegevens kunnen worden verwerkt in de nieuwsbrief van DCo.

Voor een activiteit is dus niet altijd te bepalen wanneer welke grondslag van toepassing is. Dit is extra lastig omdat er (zoals benoemd onder vraag 1) momenteel binnen Defensie duidelijke kaders en richtlijnen ontbreken voor het gebruik van de grondslag gerechtvaardigd belang voor typische bedrijfsmatige activiteiten.

²¹ Zie artikel 6 lid 1 sub f AVG. De laatste volzin van dit artikel bepaalt: "De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken."

4. Voldoet de verwerking aan de cumulatieve voorwaarden voor gerechtvaardigd belang én valt de belangenafweging ook in het voordeel van de overheidsinstelling uit?

Als er bij een activiteit sprake is van een typisch bedrijfsmatige handeling, dan moet voor toepassing van de grondslag gerechtvaardigd belang éérst ook de gerechtvaardigd belang toets worden uitgevoerd. Bij deze toets wordt er getoetst aan de drie cumulatieve vereisten van artikel 6 lid 1 sub f AVG:

1. het belang moet gerechtvaardigd zijn als rechtsbelang;
2. de verwerking van persoonsgegevens moet noodzakelijk zijn om dit belang te behartigen; en
3. er moet een belangenafweging worden gemaakt tussen de belangen van de verwerkingsverantwoordelijke en de belangen van betrokkene.

Nadat de gerechtvaardigd belangtoets is uitgevoerd en de uitkomst daarvan positief is, moet elke verwerking van persoonsgegevens ook voldoen aan de beginselen van artikel 5 AVG.

4.3 Activiteiten

In deze paragraaf worden de beoordeelde activiteiten, de mogelijke knelpunten en aanbevelingen kort beschreven. Voor een volledige omschrijving van elke activiteit, de toets van de activiteit aan de AVG beginselen en de bijbehorende mogelijke knelpunten en aanbevelingen wordt verwezen naar *Bijlage 1* van dit rapport. In *Bijlage 2* van dit rapport is per activiteit opgenomen welke persoonsgegevens er kunnen worden verwerkt.

Activiteit 1: Directie Communicatie monitort, signaleert en duidt mediaberichten

Activiteit 1 De Newsroom van de Directie Communicatie van de Bestuursstaf. Deze activiteit vond plaats tijdens het onderzoek.	
Korte beschrijving activiteit De Directie Communicatie (hierna: DCo) monitort, signaleert en duidt mediaberichten voor communicatiedoeleinden, zodat de top van Defensie, de minister en de staatssecretaris op de hoogte zijn van wat er speelt in de maatschappij rondom Defensie.	
Kwalificatie Deze activiteit valt onder de bedrijfsvoering van het Ministerie van Defensie. De vraag is echter of het verwerken van persoonsgegevens in een Nieuwsupdate en/of Nieuwsbrief ook kwalificeert als bedrijfsvoering in de zin van artikel 6 lid 1 sub f van de Algemene verordening gegevensbescherming (hierna: AVG). Overheidsinstanties kunnen namelijk alleen een beroep doen op artikel 6 lid 1 sub f AVG bij typisch bedrijfsmatige handelingen van die overheidsinstanties. In de literatuur en rechtspraak is het begrip 'typisch bedrijfsmatige handeling' onvoldoende uitgewerkt. Hierdoor kunnen wij niet beoordelen of het verwerken van persoonsgegevens in een Nieuwsupdate en/of Nieuwsbrief kan worden aangemerkt als een typisch bedrijfsmatige handeling van Defensie. Voor zover Defensie van oordeel is dat dit niet het geval is, dan kan deze activiteit alleen doorgang vinden door een beroep te doen op artikel 6 lid 1 sub e AVG. Voor een succesvol beroep daarop is echter wel een wet in formele zin vereist, waarin een taakomschrijving staat die voldoende concreet en voorzienbaar is, zodat betrokkenen uit die taakomschrijving kan afleiden dat er persoonsgegevens kunnen worden verwerkt bij het uitvoeren van die taak door de overheidsinstantie.	
Conclusie Het is onduidelijk of de Newsroom van DCo over een grondslag beschikt om persoonsgegevens te verwerken in een Nieuwsupdate en/of Nieuwsbrief. Alvorens een succesvol beroep kan worden gedaan op artikel 6 lid 1 sub f AVG, moet Defensie eerst onderzoeken of deze activiteit als een typisch bedrijfsmatige handeling kwalificeert voor een overheidsinstantie als Defensie. Voor zover Defensie van mening is dat dat niet het geval is, is de verwerking van persoonsgegevens in een Nieuwsupdate en/of Nieuwsbrief alleen rechtmatig, wanneer het verwerken van persoonsgegevens voldoende concreet en voorzienbaar blijkt uit een taakomschrijving die is neergelegd in een wet in formele zin.	

Naast het mogelijke knelpunt omtrent de rechtmatigheid van de verwerking, hebben wij ook enkele mogelijke knelpunten gesignaleerd die betrekking hebben op andere beginselen uit artikel 5 AVG. Daarom krijgt deze activiteit de kleur oranje.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Voor een mogelijk succesvol beroep op artikel 6 lid 1 sub e AVG ontbreekt een duidelijke, nauwkeurige en voorspelbare taakomschrijving, welke is vastgelegd in een wet in formele zin.	Het formuleren van een duidelijke, nauwkeurige en voorspelbare taakomschrijving voor het verwerken van persoonsgegevens door DCo en deze taakomschrijving vastleggen in een wet in formele zin.
2.	Voor een mogelijk succesvol beroep op artikel 6 lid 1 sub f AVG ontbreekt een eenduidige definitie van wat een typisch bedrijfsmatige handeling van een overheidsinstantie precies inhoudt. Mogelijk valt deze activiteit aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie, al moet hiervoor wel een belangenafweging conform artikel 6 lid 1 sub f AVG worden uitgevoerd.	Het opstellen van een beleidsstuk waarin wordt vastgelegd wat volgens Defensie wordt aangemerkt als een typisch bedrijfsmatige handeling. Indien dat nader is uitgekristalliseerd vereist artikel 6 lid 1 sub f AVG nog een belangenafweging voor het verwerken van persoonsgegevens in deze activiteit.
3.	Betrokkenen zijn mogelijk te weinig geïnformeerd over de (sociale) mediamonitoring door DCo.	Het toevoegen van een passage over (sociale) mediamonitoring in de privacyverklaring.
4.	De verwerking van persoonsgegevens uit reeds openbare mediaberichten in de Nieuwsupdate en Nieuwsbrief ontbreekt in het verwerkingenregister.	Het opnemen van een verwerking in het verwerkingenregister.
<i>Organisatorisch</i>		
5.	Het kan voorkomen dat rectificaties niet (tijdig) worden gesignaleerd, waardoor de informatievoorziening op	Het plaatsen van een disclaimer bij mediaberichten, waarin wordt aangegeven dat het mediabericht te

	onjuiste of onvolledige informatie is gebaseerd.	allen tijde onderhevig kan zijn aan rectificaties; Extra aandacht besteden aan berichten met een hoge nieuws waarde voor eventuele rectificaties.
--	--	--

Activiteit 2: Directie Communicatie verwerkt persoonsgegevens van burgers die vragen stellen via sociale media

Activiteit 2 De Newsroom van de Directie Communicatie van de Bestuursstaf. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit De Directie Communicatie (hierna: DCo) verwerkt persoonsgegevens van burgers die vragen stellen via de corporate sociale mediakanalen van Defensie met als doel het onderhouden van contact met de vraagsteller en het bereiken van het beoogde doel van vraagsteller.		
Kwalificatie Deze activiteit valt onder de bedrijfsvoering van het Ministerie van Defensie. Onderdeel van de bedrijfsvoering is het beantwoorden van publieksvragen die binnenkomen via de corporate sociale mediakanalen van Defensie. De verwerking van persoonsgegevens hierbij kan enerzijds plaatsvinden op basis van toestemming en anderzijds op basis van het gerechtvaardigd belang, omdat er sprake is van een typisch bedrijfsmatige handeling.		
Conclusie De Newsroom van DCo kan voor de verwerking van persoonsgegevens een enerzijds beroep doen op toestemming, mits de toestemming ondubbelzinnig is en door middel van een actieve handeling is gegeven. Anderzijds zijn wij van mening dat DCo ook een beroep kan doen op het gerechtvaardigd belang, mits de belangenafweging in het voordeel uitvalt van Defensie en deze belangenafweging is vastgelegd. Ten aanzien van de overige beginselen uit artikel 5 van de Algemene verordening gegevensbescherming (hierna: AVG) hebben wij enkele mogelijke knelpunten gesignaleerd. Daarom krijgt deze activiteit de kleur oranje.		
Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het is ons opgevallen dat er geen ondubbelzinnige, actieve handeling vooraf gaat aan het stellen van een vraag via de corporate sociale mediakanalen van Defensie. Hierdoor is het voor de betrokkene mogelijk onvoldoende duidelijk welke	Zorg dat de betrokkene wordt geïnformeerd over de verwerking. Het eisen van een actieve handeling van de betrokkene kan hiervoor een invulling zijn.

	persoonsgegevens voor welk doel worden verwerkt.	
2.	De vereiste belangenafweging voor een succesvol beroep op artikel 6 lid 1 sub f AVG is niet uitgevoerd.	Het uitvoeren van de vereiste belangenafweging.
3.	Het is onvoldoende duidelijk dat de privacyverklaring ook betrekking heeft op het afhandelen van vragen, klachten en verzoeken (inclusief inzagerecht) die binnenkomen op de corporate (sociale) mediakanalen van Defensie.	Het toevoegen van nieuwe passages in de privacyverklaring of het aanpassen van de huidige privacyverklaring met betrekking tot de verwerking van persoonsgegevens in relatie tot het afhandelen van vragen, klachten en verzoeken (inclusief inzagerecht) die binnenkomen op de corporate (sociale) mediakanalen van Defensie.
4.	Het verwerken van persoonsgegevens die niet relevant zijn voor de beantwoording van de gestelde vraag en bijvoorbeeld uit de vraagstelling van de betrokkene voortvloeien.	Het plaatsen van een disclaimer op de corporate sociale mediakanalen, waarin staat dat vraagsteller geen irrelevante (bijzondere) persoonsgegevens moet verstrekken.
5.	De verwerking van persoonsgegevens in deze activiteit is nog niet expliciet terug te vinden in het verwerkingsregister van Defensie.	Het publiceren van activiteit M1739 in het verwerkingenregister van Defensie.
6.	Uit de selectielijst blijkt niet duidelijk onder welke categorie de persoonsgegevens vallen die worden verwerkt in het kader van binnenkomende vragen op de corporate sociale mediakanalen van Defensie.	Concretiseren onder welke categorie de persoonsgegevens vallen en verantwoorden waarom aansluiting wordt gezocht bij die bewaartermijn.
<i>Organisatorisch</i>		
7.	<i>Organisatorisch</i> Onduidelijk is of de bewaartermijnen uit de selectielijsten ook daadwerkelijk worden gehanteerd.	Een werkinstructie opstellen ten aanzien van het verwijderen van beantwoorde vragen, zodat aan de bewaartermijnen wordt voldaan.

Activiteit 3: Defensie Cyber Commando wil een AI ontwikkelen om sociale structuren in kaart te brengen

Activiteit 3 J2 Defensie Cyber Commando. Deze activiteit vond plaats tijdens het onderzoek.	
Korte beschrijving activiteit Defensie Cyber Commando (hierna: DCC) ontwikkelt een algoritme dat netwerken en verbanden in kaart kan brengen. Dit wordt Social Network Analysis (hierna: SNA) genoemd. Het doel is om door middel van de Artificial Intelligence (hierna: AI) sociale structuren in kaart te brengen en uitlatingen te analyseren om zo groepen - en belangrijke personen binnen die groepen en hun sociale status - te identificeren. Daarbij ligt de focus op het in beeld brengen van actoren die bepaalde boodschappen uitzenden. Ook stelt de AI vast hoe er binnen het netwerk op de uitlating wordt gereageerd. Een algoritme is in principe niet meer dan een automatisch stappenplan dat door de computer wordt doorlopen. Een AI is een systeem dat is gebaseerd op machine learning. Dat wil zeggen dat een AI wordt getraind op basis van algoritmes en grote hoeveelheden voorbeelddata. Hierdoor kan de computer uiteindelijk zelfstandig taken uitvoeren. ²² DCC is de ontwikkelaar van de AI en is uiteindelijk niet de (eind)gebruiker. Als eindgebruiker zijn voorzien: ofwel andere Defensie-eenheden ten behoeve van de uitvoering van een militaire operatie in het buitenland, ofwel ondersteuning aan de politie bij een bijstandsaanvraag onder artikel 58 Politiewet 2012. Op dit moment verwerkt DCC geen persoonsgegevens in het kader van deze activiteit. DCC is zich ervan bewust dat er geen grondslag aanwezig is om persoonsgegevens te mogen verwerken en doet dat daarom ook niet.	
Kwalificatie Deze activiteit valt niet eenduidig aan te merken als interne bedrijfsvoering of onder inzet of gereedstelling. In het geval dat de AI wel wordt ingezet dan valt dit onder inzet of gereedstelling.	
Conclusie Bij de ontwikkeling van de AI - en in het verlengde daarvan bij deze activiteit - worden geen persoonsgegevens verwerkt. Inmiddels is namelijk besloten om zelf (fictieve) datasets te creëren en verder af te zien van het zoeken naar	

²² Voor meer informatie over algoritmes en AI zie: *Toezicht op AI & Algoritmes (Autoriteit Persoonsgegevens)*. Dit document is raadpleegbaar via de website van de Autoriteit Persoonsgegevens.

beschikbare datasets. Mocht in de toekomst blijken dat de wens bestaat om de AI te trainen met persoonsgegevens dan ontbreekt hiervoor momenteel een grondslag.

Eventuele toekomstige inzet van de AI zou kunnen plaatsvinden in het kader van een militaire operatie in het buitenland of onder aansturing, gezag en verantwoordelijkheid van de Minister van Justitie en Veiligheid.

Omdat er geen persoonsgegevens (zullen) worden verwerkt bij deze activiteit krijgt deze activiteit de kleur groen.

Activiteit 4: Defensie Cyber Commando zet cyberreservisten in

Activiteit 4		
Defensie Cyber Commando. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit		
Met enige regelmaat ontvangt het Defensie Cyber Commando (hierna: DCC) verzoeken voor militaire bijstand van civiele autoriteiten. In dat kader zet DCC, naast regulier militair personeel, soms ook reservepersoneel in uit de bij DCC gecentraliseerde pool van "cyberreservisten". Dit zijn reservisten met specifieke ICT-expertise. Reservisten zijn personen die normaal gesproken werkzaam zijn buiten Defensie en op vrijwillige basis worden opgeroepen door Defensie om tijdelijk bepaalde werkzaamheden te verrichten. Tijdens de oproep/uitvoering van werkzaamheden hebben deze reservisten de status van militair. Bij ondersteuning van civiele autoriteiten ligt de verantwoordelijkheid voor de eventuele verwerking van persoonsgegevens bij de aanvragende autoriteit.		
Kwalificatie		
Deze activiteit is niet te kwalificeren als interne bedrijfsvoering of gereedstelling. Op het moment dat er cyberreservisten worden ingezet is sprake van inzet.		
Conclusie		
Bij deze activiteit verwerkt DCC geen persoonsgegevens. Op het moment dat cyberreservisten persoonsgegevens verwerken ligt de verantwoordelijkheid bij de civiele autoriteit. Daarom krijgt deze activiteit de kleur groen.		
Mogelijke knelpunten		Aanbevelingen
<i>Organisatorisch</i>		
1.	Cyberreservisten kunnen mogelijk baat hebben bij (meer, in tegenstelling tot ad hoc) structurele kennis van privacy.	Op het moment dat cyberreservisten over te weinig privacy kennis beschikken, is het raadzaam om structureel privacy trainingen te verzorgen voor de cyberreservisten. Momenteel worden cyberreservisten ad hoc gebriefd over wat zij wel en niet mogen doen als er persoonsgegevens worden verwerkt bij een project waarbij zij worden ingezet. Toch is het raadzaam om periodiek privacy trainingen te geven.

Activiteit 5A: De Genie levert militaire bijstand aan civiele autoriteiten

Activiteit 5A

Genie – Leveren militaire bijstand aan civiele autoriteiten. Deze activiteit vond plaats tijdens het onderzoek.

Korte beschrijving activiteit

Met enige regelmaat ontvangt Defensie verzoeken voor militaire bijstand van civiele autoriteiten. Deze activiteit gaat in op ondersteuning door Defensie middels eenheden of teams met specifieke expertise, onder andere door:

- CBRN Respons Eenheid (hierna: CBRN RE): De CBRN RE staat dag en nacht paraat om civiele hulpdiensten bij eventuele CBRN dreigingen en incidenten advies en ondersteuning te bieden. De CBRN RE detecteert, identificeert en ontsmet met specialistische apparatuur. Waar nodig wordt ook geadviseerd over mogelijke neutralisatie van stoffen. Dit vindt plaats in het fysieke domein. De CBRN RE verzamelt data van en over stoffen om hier aansluitend een advies op te geven of mogelijk actie op te plannen. Hierbij worden geen persoonsgegevens verwerkt.
- Advanced Search Teams (hierna: AST): Dit zijn zoekteams met specialisten en apparatuur van Defensie, bestaande uit militairen met kennis en ervaring, opgedaan tijdens missies en operaties in het buitenland - en Nederland zelf - over het onderkennen en doorzoeken van het gehele fysieke domein. Hierbij worden geen persoonsgegevens verwerkt; het gaat enkel om lezen met sensoren. De civiele autoriteit aan wie bijstand of ondersteuning wordt verleend (veelal justitie) bepaalt waar het AST naar zoekt. De specialisten van het AST komen voort uit alle krijgsmachtdelen en zijn dus niet specifiek gelieerd aan de Genie. Voor het samenstellen van een AST wordt gecoördineerd tussen de Directie Operaties en het uitvoerende krijgsmachtonderdeel.

Defensie verwerkt doorgaans geen persoonsgegevens (behoudens NAW-gegevens van Defensiepersoneel) in het kader van militaire bijstand of MSOB. AST's en/of genisten van CBRN RE verwerken in sommige gevallen wel persoonsgegevens, bijvoorbeeld in het kader van ondersteuning van een strafrechtelijk onderzoek. Dit valt onder verantwoordelijkheid van een de civiele autoriteit. De civiele autoriteit bepaalt waar naar wordt gezocht en bepaalt daarmee het doel en de middelen van de verwerking. Defensie is dus in het kader van militaire bijstand niet aan te merken als verwerkingsverantwoordelijke.

<p>N.B.</p> <p>Er zijn ook andere ontwikkelingen besproken tijdens het interview over deze activiteit. Deze ontwikkelingen vonden deels of nog niet plaats tijdens het onderzoek en vallen buiten scope van het onderzoek, maar zijn voor de volledigheid opgenomen in de laatste paragraaf (na de conclusie) van de uitgebreide activiteitsomschrijving (<i>Bijlage 1</i>). Deze ontwikkelingen beïnvloeden de kleurcodering van deze activiteit echter niet.</p>		
<p>Kwalificatie</p> <p>De Genie valt onder de krijgsmacht. Deze activiteit valt te kwalificeren als inzet op het moment dat de Genieonderdelen (CBRN RE of het AST) worden ingezet.</p>		
<p>Conclusie</p> <p>Het leveren van militaire bijstand/MSOB aan civiele autoriteiten die de CBRN RE en AST's uitvoeren kan in de huidige vorm doorgaan. De verwerking van persoonsgegevens vindt plaats onder verantwoordelijkheid van de civiele autoriteit. Er zijn mogelijke knelpunten gesignaleerd bij zowel militaire bijstand/MSOB. Deze blokkeren de doorgang van de het leveren van militaire bijstand/MSOB echter niet direct. Daarom krijgt deze activiteit de kleur groen.</p>		
Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	<p>De respondent heeft aangegeven dat AST's aan de hand van dataverzameling en bijbehorende analyse mogelijk een grotere bijdrage kunnen bieden. AST's zijn in staat om een variëteit aan data te verzamelen. Dit kan data zijn van:</p> <ul style="list-style-type: none"> • foto's; • artikelen waar mogelijke biometrie (sigaretten, bekers etc) op zit; • of de biometrische gegevens zelf door het verzamelen van vingerafdrukken, haar, nagels enzovoort. <p>Deze mogelijke extra bijdrage vond tijdens het onderzoek niet plaats, omdat hulpdiensten (politie) dit momenteel zelf uitvoeren. Defensie heeft dus</p>	<p><i>Formeel wettelijke grondslag</i></p> <p>Het is aan de wetgever om wetgeving te creëren voor overheidsorganisaties waaruit taken en bevoegdheden zijn te ontlelen. Deze taken en bevoegdheden moeten daarbij voldoende duidelijk en concreet zijn om te kwalificeren als grondslag in de zin van artikel 6 lid 1 sub e AVG. Het is daarom aan de wetgever om te bepalen of het wenselijk is dat de AST's deze en/of soortgelijke activiteiten uitvoert. Wij adviseren in ieder geval om de taken en bijbehorende bevoegdheden op een heldere en voor de betrokkene duidelijke wijze vast te leggen in (formele) wetgeving waarbij de beginselen van de AVG in acht worden genomen.</p>

	geen zelfstandige grondslag of mandaat om persoonsgegevens te verwerken en wellicht van grotere betekenis te kunnen zijn.	
<i>Organisatorisch</i>		
2.	<p>De respondent geeft aan dat veiligheid van eigen personeel (CBRN RE & AST's) een mogelijk knelpunt is. De gegevens- en identiteitsbescherming van eigen Defensiepersoneel tijdens het uitvoeren van operaties in het nationale domein is mogelijk onvoldoende gewaarborgd. Het gaat namelijk om (relatief, rond de 60 Fte) kleine teams met hele specifieke kennis. Tijdens deze acties kunnen omstanders of bewoners van objecten dicht bij een AST komen. Het is daarom tijdens een ondersteuningsactie bij de politie (bijvoorbeeld gericht op het doorzoeken van een huis op verborgen ruimtes om bewijslast te vinden) lastig om anoniem te blijven.²³</p> <p>Er bestaat mogelijk een spanningsveld tussen wat eenheden willen – bescherming persoonlijke levenssfeer van personeel – en Defensie, zij wil laten zien welke specialistische kennis zij in huis heeft.²⁴</p>	<p>Onderzoek de mogelijkheden en wenselijkheid om bij militaire bijstand door de CBRN RE en AST's het defensiepersoneel (onzichtbaar) te laten 'mengen' met de hulpdiensten ter plaatse. Bijvoorbeeld door het dragen van hetzelfde uniform. Respondent heeft aangegeven dat hier eerder over is nagedacht, maar niet is toegepast. Om te voorkomen dat de aandacht wordt getrokken - bijvoorbeeld door het gebruik van gezichtsbedekkende attributen - lijkt dit ons een potentieel werkbare oplossing.</p>

²³ Zie ook: <https://magazines.defensie.nl/defensiekrant/2015/07/op-pad-met-het-zoekteam-van-de-landmacht>.

²⁴ Zie bijvoorbeeld de volgende nieuwsberichten: <https://magazines.defensie.nl/defensiekrant/2015/07/op-pad-met-het-zoekteam-van-de-landmacht>; en: Specialistische zoekteams Defensie vinden bewijsmateriaal in drugszaak | Nieuwsbericht | Defensie.nl.

Activiteit 5B: Om Advanced Search Teams voor te bereiden ten behoeve van de algemene gereedstelling wordt gebruikgemaakt van realistische oefenscenario's

Activiteit 5B Genie – Trainen en opleiden Advanced Search Teams (hierna: AST) Deze activiteit vond plaats tijdens het onderzoek.	
Korte beschrijving activiteit De AST's zijn zoekteams met specialisten en apparatuur van Defensie, bestaande uit militairen met kennis en ervaring, opgedaan tijdens missies en operaties in het buitenland – en in Nederland zelf – over het onderkennen en doorzoeken van het gehele fysieke domein onder complexe omstandigheden. Ten behoeve van de algemene gereedstelling op inzet (bescherming eigen grondgebied en dat van bondgenoten, hoofdtak 1) en het ondersteunen van civiele autoriteiten (o.a. militaire bijstand of MSOB, hoofdtak 3) wordt onder meer gebruikgemaakt van realistische 'scenario's'. Daarvoor bestaat onder andere het Opleidings- en Trainingscentrum Genie. De noodzaak en het doel zijn gelegen in het zo realistisch mogelijk oefenen, vergelijkbaar met een daadwerkelijke inzet.	
Kwalificatie AST's vallen onder de krijgsmacht. Deze activiteit valt te kwalificeren als gereedstellen.	
Conclusie Het wordt noodzakelijk geacht (of in ieder geval wenselijk) om persoonsgegevens te verwerken ten behoeve van de algemene gereedstelling tijdens het trainen en opleiden om dit zo realistisch mogelijk te maken. Er is echter waarschijnlijk enkel een grondslag om <u>gewone</u> persoonsgegevens van eigen Defensiepersoneel te verwerken tijdens training en opleiding. Er lijkt geen grondslag te bestaan om gewone, bijzondere en/of gevoelige persoonsgegevens te verwerken van omstanders of burgers ten behoeve van een oefening in het kader van algemene gereedstelling. Onze aanbevelingen strekken tot het onderzoeken van de mogelijkheid van een formeel wettelijke grondslag, het verrichten van nader onderzoek naar typisch bedrijfsmatige handelingen voor een overheidsinstantie of tot het gebruik van een virtuele oefenomgeving en fictieve datasets. Er ontbreekt mogelijk een sluitende grondslag om persoonsgegevens te verzamelen, terwijl dit in het kader van de algemene gereedstelling wel plaatsvindt. Daarom krijgt deze activiteit de kleur oranje.	
Mogelijk knelpunt	Aanbeveling
<i>Juridisch</i>	

1.	<p>Ondanks het bestaan van een Opleidings- en Trainingscentrum Genie waar het mogelijk is om realistische scenario's na te bootsen zonder het gebruik van persoonsgegevens. Echter kunnen er tijdens oefeningen mogelijk persoonsgegevens worden verwerkt. In het verlengde daarvan zijn er vragen gesteld in welke gevallen dat is toegestaan en binnen welke kaders. Het wordt als gemis ervaren dat een grondslag ontbreekt om persoonsgegevens te verwerken ten behoeve van de algemene gereedstelling. Het gaat dan om het verwerken van persoonsgegevens in het kader van informatie gestuurd optreden (hierna: IGO).</p>	<p><i>Formeel wettelijke grondslag</i></p> <p>Het is aan de wetgever om wetgeving te creëren voor overheidsorganisaties waaruit taken en bevoegdheden zijn te ontlelen. Deze taken en bevoegdheden moeten daarbij voldoende duidelijk en concreet zijn om te kwalificeren als grondslag in de zin van artikel 6 lid 1 sub e AVG. Het is daarom aan de wetgever om te bepalen of het wenselijk is dat AST's deze en/of soortgelijke activiteiten uitvoert. Wij adviseren in ieder geval om de taken en bijbehorende bevoegdheden op een heldere en voor de betrokkene duidelijke wijze vast te leggen in (formele) wetgeving waarbij de beginselen van de AVG in acht worden genomen.</p> <p><i>Verricht nader onderzoek naar de reikwijdte van typisch bedrijfsmatige handelingen</i></p> <p>Het is de vraag of de gewenste verzameling van persoonsgegevens ten behoeve van training en opleiding is aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie. Als dit namelijk het geval is dan zou een beroep op het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG) mogelijk zijn, mits de verwerking gerechtvaardigd en noodzakelijk is en er een belangenafweging is uitgevoerd en aan de overige eisen van de AVG (in het bijzonder artikel 5 AVG) wordt voldaan. Het belang van Defensie moet hierbij wel prevaleren boven het belang van de betrokkene. Omdat in de wet- en regelgeving, rechtspraak en literatuur geen duidelijke definitie is gegeven van een typisch</p>
----	---	--

	<p>bedrijfsmatige handeling van een overheidsinstantie, is het lastig om te beoordelen of bij deze activiteit een beroep mogelijk is op het gerechtvaardigd belang.</p> <p><i>Virtuele oefenomgeving</i> Het lijkt (technisch en praktisch) vrijwel onmogelijk om een realistisch virtueel oefenscenario te creëren. Door deze gepercipieerde onmogelijkheid zijn AST's mogelijk niet in staat om te trainen voor zover het gaat om oefenen waarbij informatie die te herleiden is naar een persoon – bijvoorbeeld biometrische gegevens – in voorkomt.</p> <p>Ontwikkelingen in de techniek volgen elkaar desalniettemin wél snel op. Het is zinvol om nader onderzoek te doen naar mogelijkheden en resultaten van het oefenen met gecreëerde oefenscenario's²⁵ en fictieve datasets.</p>
--	---

²⁵ Zie ook Reactie op verzoek commissie over oefenmogelijkheden voor informatiegestuurd optreden, Tweede Kamer, vergaderjaar 2021–2022, 32 761, nr. 203, p. 3-4.

Activiteit 6: Land Information Manoeuvre Centre wil aan de hand van data science technieken (toekomstig) handelingsperspectief ontwikkelen

Activiteit 6		
Land Information Manoeuvre Centre. Deze activiteit vond niet plaats tijdens het onderzoek.		
Korte beschrijving activiteit Het Land Information Manoeuvre Centre (hierna: LIMC) wil aan de hand van onder meer Artificial Intelligence (hierna: AI) en data science toekomstig handelingsperspectief ontwikkelen. Dit in het kader van informatie gestuurd optreden (hierna: IGO). Daarbij kijkt LIMC naar fenomenen en volgt LIMC dus geen personen. Het verzamelen van informatie richt zich daarbij op het gehele omgevingsbeeld. Daarbij gaat het om inzicht vergaren in trends, ontwikkelingen en fenomenen. De informatie die LIMC verzamelt is afhankelijk van de onderzoeksvraag. Bij deze activiteit wordt gekeken naar de gewenste activiteiten die LIMC wilde uitvoeren. Dat gaat dus verder dan de uitgevoerde activiteiten gedurende de coronapandemie. Let op: de activiteiten van LIMC liggen sinds november 2020 stil en medio april 2022 is besloten om in de nabije toekomst niets meer te doen met het Concept Development & Experimentation (hierna: CD&E) traject. Momenteel houdt LIMC zich enkel bezig met de ontwikkeling van doctrine en kennisontwikkeling. Daarbij verwerkt LIMC geen persoonsgegevens. Het interview heeft plaatsgevonden op 28 januari 2022.		
Kwalificatie LIMC valt onder de krijgsmacht. Deze activiteit valt te kwalificeren als inzet/gereedstellen en niet als een activiteit die samenhangt met of ondersteunt aan de bedrijfsvoering.		
Conclusie Momenteel is er bij deze activiteit geen grondslag om persoonsgegevens te verwerken tijdens het trainen en gedurende de algemene gereedstelling. Zolang er geen grondslag is om persoonsgegevens te verwerken kunnen en mogen de gewenste activiteiten niet plaatsvinden. Daarom krijgt de gewenste activiteit de kleur rood.		
Mogelijke knelpunten		Aanbevelingen
Juridisch		
1.	LIMC heeft geen zelfstandige grondslag om persoonsgegevens te verwerken tijdens het trainen en de algemene gereedstelling.	<i>Gesimuleerde omgevingen</i> Indien dit als knelpunt wordt ervaren is het een mogelijkheid om meer onderzoek te doen naar fictieve

		<p>datasets en het creëren van gesimuleerde omgevingen met fictieve data/persoonsgegevens.</p> <p><i>Formeel wettelijke grondslag</i></p> <p>Het is aan de wetgever om wetgeving te creëren voor overheidsorganisaties waaruit taken en bevoegdheden zijn te ontlelen. Deze taken en bevoegdheden moeten daarbij voldoende duidelijk en concreet zijn om te kwalificeren als grondslag in de zin van artikel 6 lid 1 sub e AVG. Het is daarom aan de wetgever om te bepalen of het wenselijk is dat LIMC deze en/of soortgelijke activiteiten uitvoert. Wij adviseren in ieder geval om de taken en bijbehorende bevoegdheden op een heldere en voor de betrokkene duidelijke wijze vast te leggen in (formele) wetgeving waarbij de beginselen van de AVG in acht worden genomen.</p>
<i>Organisatorisch</i>		
1.	<p>Defensieonderdelen kunnen een informatieverzoek indienen bij de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). Het is niet bekend of de MIVD aan verzoeken voldoet die toezien op het aanleveren van de informatie die LIMC wil verzamelen. Ook is onbekend onder welke voorwaarden de MIVD een informatieverzoek beantwoordt.</p>	<p>Op het moment dat dit als knelpunt wordt ervaren zou het mogelijk een oplossing zijn om de samenwerking tussen de MIVD en andere Defensieonderdelen te (her)evalueren.</p>

Activiteit 7: Commando Luchtstrijdkrachten wil door middel van simpele zoekopdrachten dreigingen onderzoeken

<p>Activiteit 7</p> <p>Commando Luchtstrijdkrachten. Deze activiteit vond niet plaats tijdens het onderzoek.</p>	
<p>Korte beschrijving activiteit</p> <p>De Commando Luchtstrijdkrachten (hierna: CLSK) wil capaciteit hebben die zich bezighoudt met het verrichten van simpele zoekacties op internet om zo eventuele dreigingen te onderzoeken. Onder simpele zoekactie wordt bijvoorbeeld verstaan het op internet zoeken met de zoektermen 'Vliegbasis X' in combinatie met een bepaalde dreiging. Daarbij wil CLSK betogingen of TESSOC-activiteiten (Terrorism Espionage Subversion Sabotage Organised Crime) tijdig detecteren. CLSK wil eventuele dreigingen vooral kunnen duiden. Als de conclusie is dat er concrete dreigingen zijn wordt de politie daarvan op de hoogte gebracht en kan CLSK eventueel maatregelen treffen. Het doel van deze potentiële activiteit is uitdrukkelijk niet om persoonsgegevens te verwerken, maar het verwerken van persoonsgegevens als 'bijvangst' is onvermijdelijk. Op dit moment wordt deze activiteit niet uitgevoerd, omdat onduidelijk is welke activiteiten security medewerkers in verband met de Algemene verordening gegevensverwerking (hierna: AVG) mogen uitvoeren. Het grootste deel van de beveiligingstaken wordt uitgevoerd door Defensie Bewakings- en Beveiligingsorganisatie (hierna: DBBO), maar een deel voert CLSK zelf uit.</p>	
<p>Kwalificatie</p> <p>Deze potentiële activiteit is mogelijk te kwalificeren als interne bedrijfsvoering. Het verrichten van simpele zoekacties op internet om mogelijke dreigingen te onderzoeken, ziet toe op de beveiliging van vliegbases, luchtmachtonderdelen en personen van CLSK. Een overheidsinstantie kan alleen een beroep doen op het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG), als sprake is van een typisch bedrijfsmatige handeling. Een voorbeeld van een typisch bedrijfsmatige handeling van overheidsinstanties is het beveiligen van gebouwen. Dit wijkt namelijk niet af van private organisaties. Bij deze activiteit gaat het om het beveiligen van vliegbases en luchtmachtonderdelen door het verrichten van zoekacties in het digitale domein. Het is lastig om te beoordelen wat een typisch bedrijfsmatige handeling van een overheidsinstantie precies inhoudt. In de wet- en regelgeving, de literatuur en de rechtspraak is namelijk geen duidelijke definitie gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie. Daarom is het onduidelijk of daar bij deze potentiële activiteit sprake van is. Om de activiteit doorgang te laten vinden moet eerst</p>	

onderzocht worden of dit een typisch bedrijfsmatige handeling is van een overheidsinstantie. Als de conclusie is dat dit geen typisch bedrijfsmatige handeling is en er geen sprake is van een gerechtvaardigd belang, kan deze potentiële activiteit enkel doorgang vinden indien er een formeel wettelijke grondslag wordt gecreëerd.

Conclusie

Voordat deze potentiële activiteit kan plaatsvinden moet onderzoek worden verricht naar of deze activiteit is te kwalificeren als een typisch bedrijfsmatige handeling van een overheidsinstantie. Op het moment dat er sprake is van een typisch bedrijfsmatige handeling moet er ook een belangenafweging plaatsvinden tussen het belang van Defensie en het belang van de betrokkene, de gerechtvaardigd belang-toets. Als de conclusie is dat dit geen typisch bedrijfsmatige handeling is van een overheidsinstantie en een beroep op de grondslag van het gerechtvaardigd belang daarmee niet open staat, kan deze potentiële activiteit enkel doorgang vinden indien er een formeel wettelijke grondslag wordt gecreëerd. Er moet dus nader onderzoek worden gedaan naar de grondslag. Daarom krijgt deze activiteit de kleur oranje.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het is onduidelijk of er een grondslag is om deze potentiële activiteit te ontplooiën.	<p><i>Typisch bedrijfsmatige handeling</i> Verricht nader onderzoek of deze potentiële activiteit is te kwalificeren als een typisch bedrijfsmatige handeling van een overheidsinstantie. Indien dit het geval is, dan zou er mogelijk een grondslag (artikel 6 lid 1 sub f AVG gerechtvaardigd belang) zijn om de activiteit uit te voeren.</p> <p><i>Formeel wettelijke grondslag</i> Mocht er geen sprake zijn van een typisch bedrijfsmatige handeling dan kan de potentiële activiteit enkel plaatsvinden als er een formeel wettelijk grondslag wordt gecreëerd.</p>
<i>Organisatorisch</i>		
2.	Er is onvoldoende capaciteit binnen CLSK die zich bezighoudt met privacyvraagstukken. Hierdoor is er een grote achterstand op het gebied van	Zorg voor meer capaciteit of zorg ervoor dat meer medewerkers kennis hebben van de geldende wet- en regelgeving op het gebied van privacy.

	Data Protection Impact Assessments (hierna: DPIA's).	
<i>Ethisch</i>		
3.	Er is na het Land Information Manoeuvre Centre (hierna: LIMC) een angst ontstaan om persoonsgegevens te verwerken.	Vergroot de bewustwording met betrekking tot de AVG onder de medewerkers.

Activiteit 8: De Intelligence, Surveillance and Reconnaissance Division wil een scraper gebruiken om ontwikkelingen te duiden ter ondersteuning van de besluitvorming

Activiteit 8 Commando Luchtmacht. Deze activiteit vond niet plaats tijdens het onderzoek.	
Korte beschrijving activiteit Ten behoeve van de Very High Readiness Joint Task Force (hierna: VJTF) voorbereiding wil de Intelligence, Surveillance and Reconnaissance Division (hierna: ISRD) van de Commando Luchtmacht (hierna: CLSK) informatie van het internet verzamelen en verwerken door middel van een scraper. De scraper is ontwikkeld door het bedrijf Tardis Research. Tardis Research is een softwarebedrijf dat zich heeft gespecialiseerd in big data analysis solutions. Omdat er een grote hoeveelheid aan mogelijk nuttige informatie op het (openbare) internet staat die een bijdrage kan leveren aan de besluitvorming bij CLSK is deze behoefte ontstaan. De besluitvorming ziet dan met name toe op de vraag of er krijgsmachtspersoneel in het kader van de VJTF zal moeten worden uitgezonden en op welke wijze ze hierop moeten voorbereiden. De scraper doorzoekt hiervoor openbare bronnen met het doel om te duiden hoe situaties - bijvoorbeeld aan de grenzen van conflictgebieden - zich ontwikkelen. Let op: deze activiteit is momenteel niet gaande, daarom kwalificeert deze activiteit zich als 'potentiële activiteit'. Deze uitwerking ziet toe op de situatie dat de activiteit zoals is voorgelegd plaatsvindt binnen de voorgestelde kaders.	
Kwalificatie Het ISRD valt onder de krijgsmacht. Deze activiteit valt te kwalificeren als ondersteunen in de informatiebehoefte in de besluitvorming van CLSK ten behoeve van mogelijke inzet. Met dit gegeven valt de activiteit niet onder interne bedrijfsvoering. Activiteiten die samenhangen met mogelijke inzet is immers niet aan te merken als typisch bedrijfsmatige handeling van een overheidsinstantie in de zin van de Algemene Verordening Gegevensbescherming (hierna: AVG).	
Conclusie Hoewel de activiteit niet gaande is, zijn er voor eventueel toekomstig gebruik door de ISRD van CLSK mogelijk knelpunten geconstateerd die maken dat de activiteit in de huidige, voorgestelde vorm waarschijnlijk niet kan doorgaan. Op dit moment lijkt er geen verwerkingsgrondslag aanwezig te zijn, die het	

mogelijk maakt om persoonsgegevens te verwerken. Hoewel er geen intentie is om persoonsgegevens te verwerken, vindt deze verwerking waarschijnlijk onoverkomelijk plaats. Al dan niet als 'bijvangst'. Dat betekent dat de potentiële activiteit op het moment dat deze op de voorgestelde wijze wordt uitgevoerd volgens ons waarschijnlijk niet in deze vorm kan plaatsvinden. Daarom krijgt deze activiteit de kleur rood.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Voor de verwerking van persoonsgegevens in het kader van de inzet van een scraper ligt de grondslag van artikel 6 lid 1 sub e AVG, vervulling van een taak van algemeen belang, voor de hand. Hiervoor is het noodzakelijk dat de taak aan de verwerkingsverantwoordelijke, in deze Defensie, zijn opgedragen bij Europees of Nederlands recht. Het doel van de verwerking moet daarbij duidelijk zijn af te leiden uit de taakomschrijving. De grondslag om persoonsgegevens te verwerken ten behoeve van deze activiteit lijkt te ontbreken.	Het is aan de wetgever om wetgeving te creëren voor overheidsorganisaties waaruit taken en bevoegdheden zijn te ontlelen. Deze taken en bevoegdheden moeten daarbij voldoende duidelijk en concreet zijn om te kwalificeren als grondslag in de zin van artikel 6 lid 1 sub e AVG. Het is daarom aan de wetgever om te bepalen of het wenselijk is dat CLSK deze en/of soortgelijke activiteiten uitvoert. Wij adviseren in ieder geval om de taken en bijbehorende bevoegdheden op een heldere en voor de betrokkene duidelijke wijze vast te leggen in (formele) wetgeving waarbij de beginselen van de AVG in acht worden genomen.
<i>Organisatorisch</i>		
2.	Het is de verwachting dat de MIVD te weinig capaciteit en daarmee gewenste én vereiste slagkracht heeft op het moment dat het nodig is. In het geval van een conflict is de rangorde van ondersteuning (volgens de respondent) als volgt: <ol style="list-style-type: none"> 1. Politieke besluitvorming; 2. Commandant der Strijdkrachten (hierna: CDS); 3. Operationele Commando's (hierna: 	Het lijkt een onmogelijkheid om alle (relevante) informatie uit te wisselen, of mee te nemen naar het eigen krijgsmachtonderdeel. Een oplossing voor informatieachterstand(en) op het gebied van informatie gestuurd optreden (hierna: IGO) tussen krijgsmachtonderdelen is hiermee derhalve niet gegeven. In dat kader is overwogen en gesproken over de potentiële optie om Defensie (gedeeltelijk) onder de Wet op de inlichtingen- en

	<p>OPCO's, waaronder CLSK).</p> <p>Dit levert mogelijk problemen op. Het is waarschijnlijk 'te laat' als er pas informatie wordt verzameld op het moment dat de vliegtuigen al de lucht in moeten. Bovendien ontstaat daarmee een informatieachterstand ten opzichte van de tegenstander.</p>	<p>veiligheidsdiensten 2017 (hierna: Wiv2017) te laten opereren.</p> <p>De respondenten spreken de wens uit om de activiteiten onder de AVG uit te voeren. Zodat zij zelf in een eerder stadium informatie kunnen verzamelen zonder afhankelijk te zijn van de MIVD. Dit zou betekenen dat er een formeel wettelijke grondslag moet worden gecreëerd. Momenteel ontbreekt namelijk een grondslag om bij deze activiteit zelf persoonsgegevens te verwerken.</p>
--	---	---

Activiteit 9A: Het Korps Mariniers van het Commando Zeestrijdkrachten heeft de wens om met een geïntegreerd mobiel interceptieplatform signalen, afkomstig van de mobiele apparaten van de eigen mariniers, te verzamelen en te verwerken.

<p>Activiteit 9A</p> <p>Korps Mariniers van het Commando Zeestrijdkrachten. Deze activiteit vond niet plaats tijdens het onderzoek.</p>	
<p>Korte beschrijving activiteit</p> <p>Het Korps Mariniers van CZSK het Commando Zeestrijdkrachten (hierna: CZSK) heeft de wens om gebruik te maken van een geïntegreerd mobiel interceptieplatform (hierna: GMI). Het GMI verzamelt en verwerkt data door middel van Cyber and Electromagnetic Activities (hierna: CEMA). Hiermee kunnen onder andere radio-, wifi- en Bluetoothsignalen worden verwerkt. Het doel hiervan is de Operational Security (hierna: OPSEC) en de Digital Force Protection zeker te stellen en om de eigen defensiemedewerkers bewust te maken van de risico's en consequenties van de verspreiding van informatie. Met een GMI kunnen kort gezegd interne en externe risico's in kaart worden gebracht. Hierbij kunnen persoonsgegevens worden verwerkt van de eigen mariniers en van derden die (niet) aan Defensie zijn gelieerd en zich binnen het ontvangstbereik van het GMI bevinden.</p>	
<p>Kwalificatie</p> <p>Het Korps Mariniers van het CZSK valt onder de krijgsmacht en deze beoogde activiteit is te kwalificeren als gereedstellen. Alhoewel deze beoogde activiteit ook bij inzet kan worden uitgevoerd, valt dit buiten de scope van het onderzoek.</p>	
<p>Conclusie</p> <p>Het Commando Zeestrijdkrachten (hierna: CZSK) beschikt op basis van de huidige wet- en regelgeving (nog) niet over een grondslag om persoonsgegevens te mogen verwerken bij deze beoogde activiteit. Daarnaast wordt ook aan de overige beginselen uit artikel 5 AVG nog niet (volledig) voldaan. Alvorens een GMI daadwerkelijk kan worden gebruikt, is het noodzakelijk dat CZSK onder meer aandacht besteedt aan de informatieplicht, protocollen om minimale gegevens te verwerken, bewaartermijnen en het beveiligingsbeleid. Daarom krijgt deze activiteit de kleur rood.</p>	

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het ontbreken van een wettelijke grondslag waaruit een bevoegdheid kan worden ontleend om persoonsgegevens te mogen verwerken bij het gebruik van een GMI.	Het creëren van een formeel wettelijke grondslag om persoonsgegevens te verwerken voor het gebruik van een GMI.
2.	De informatieplicht uit artikel 13 AVG wordt niet volledig nageleefd.	In eenvoudige en duidelijke taal omschrijven wat het doel is van de verwerking van persoonsgegevens met een GMI, wat er met de gegevens gebeurt en de overige te verstrekken informatie zoals genoemd in artikel 13 AVG.
3.	Uit het onderzoek is ons niet gebleken dat Defensie reeds beschikt over protocollen, waarin bijvoorbeeld is vastgelegd wanneer diepgaander onderzoek naar een signaal wordt verricht.	In het kader van minimale gegevensverwerking verdient het aanbeveling om een protocol op te stellen waarin is vastgesteld wanneer een signaal als verdacht wordt aangemerkt en onder welke omstandigheden diepgaander onderzoek is toegestaan.
4.	Vooralsnog is het onbekend welke persoonsgegevens noodzakelijk zijn om het doel van het gebruik van een GMI te bereiken.	In het kader van minimale gegevensverwerking verdient het aanbeveling om in de gevallen waarbij diepgaander onderzoek naar metadata wordt gedaan, alleen die metadata te onderzoeken die noodzakelijk is om de identiteit van de betrokkene te achterhalen.
5.	Vooralsnog ontbreken specifieke bewaartermijnen voor eventuele persoonsgegevens die bij het gebruik van een GMI worden verwerkt.	Generieke bewaartermijnen vastleggen en een protocol opstellen waaruit blijkt op welke manier de vernietiging van de persoonsgegevens plaatsvindt. Indien het noodzakelijk is om persoonsgegevens langer te bewaren, dienen er aanknopingspunten te worden vastgelegd in het protocol onder welke omstandigheden langer bewaren geoorloofd is.

6.	Vooralsnog blijkt niet dat Defensie reeds heeft vastgesteld welke personen toegang kunnen krijgen tot de standalone laptop en de eventuele persoonsgegevens die daarop verwerkt zijn.	Het opstellen van een autorisatiematrix voor toegang tot de standalone laptop. Daarnaast moet worden zorggedragen voor een regelmatige update van het gehanteerde wachtwoord en eventueel voor tweefactor authenticatie voor zover dit nog niet uit het DBB volgt.
7.	De verwerking van persoonsgegevens bij deze activiteit is niet opgenomen in het verwerkingsregister van Defensie.	De verwerking van persoonsgegevens bij deze activiteit opnemen in het verwerkingsregister.
<i>Organisatorisch</i>		
8.	Vooralsnog is het onbekend wat de gevolgen zijn op het moment dat een ongewenst digitaal signaal afkomstig van een mobiel apparaat van een marinier wordt gedetecteerd.	Op het moment dat een signaal van een marinier wordt gedetecteerd, kan er voor worden gekozen om eerst in algemene zin de mariniers nogmaals dringend te verzoeken hun mobiele apparaten uit te schakelen. Wordt het signaal bij een tweede scan nogmaals geconstateerd, dan kan bijvoorbeeld worden overgegaan tot nader onderzoek, waarbij ook persoonsgegevens worden verwerkt.

Activiteit 9B: Het Korps Mariniers van het Commando Zeestrijdkrachten heeft de wens om met een geïntegreerd mobiel interceptieplatform signalen, afkomstig van de mobiele apparaten van potentiële vijanden, te verzamelen en te verwerken

Activiteit 9B Korps Mariniers van het Commando Zeestrijdkrachten. Deze activiteit vond niet plaats tijdens het onderzoek.	
Korte beschrijving activiteit Het Korps Mariniers van het Commando Zeestrijdkrachten (hierna: CZSK) heeft de wens om gebruik te maken van een geïntegreerd mobiel interceptieplatform (hierna: GMI). Het GMI verzamelt en verwerkt data door middel van Cyber and Electromagnetic Activities (hierna: CEMA). Hiermee kunnen onder andere radio-, wifi- en Bluetoothsignalen worden verwerkt. Het doel hiervan is de Operational Security (hierna: OPSEC) en de Digital Force Protection zeker te stellen en om de eigen defensiemedewerkers bewust te maken van de risico's en consequenties van de verspreiding van informatie. Met een GMI kunnen kort gezegd interne en externe risico's in kaart worden gebracht. Hierbij kunnen persoonsgegevens worden verwerkt van de eigen mariniers en van derden die niet aan Defensie zijn gelieerd en zich binnen het ontvangstbereik van het GMI bevinden.	
Kwalificatie Het Korps Mariniers van het CZSK valt onder de krijgsmacht en deze beoogde activiteit is te kwalificeren als gereedstellen. Alhoewel deze beoogde activiteit ook bij inzet kan worden uitgevoerd, valt dit buiten de scope van het onderzoek.	
Conclusie Het Commando Zeestrijdkrachten (hierna: CZSK) beschikt op basis van de huidige wet- en regelgeving (nog) niet over een grondslag om persoonsgegevens te mogen verwerken bij deze beoogde activiteit. Daarnaast wordt ook aan de overige beginselen uit artikel 5 AVG nog niet (volledig) voldaan. Alvorens een GMI daadwerkelijk kan worden gebruikt, is het noodzakelijk dat CZSK onder meer aandacht besteedt aan de informatieplicht, protocollen om minimale gegevens te verwerken, bewaartermijnen en het beveiligingsbeleid. Daarom krijgt deze activiteit de kleur rood.	

Mogelijke knelpunten		Aanbevelingen
Juridisch		
1.	Het ontbreken van een wettelijke grondslag voor het gebruik van een GMI.	Het creëren van een formeel wettelijke grondslag om persoonsgegevens te verwerken voor het gebruik van een GMI.
2.	De juridische mogelijkheid bestaat om Defensie te ontslaan van haar verplichting om betrokkenen van informatie te voorzien, mits die uitzondering voortvloeit uit een Unierechtelijke of lidstaatrechtelijke bepaling.	Wetgeving ontwerpen op basis waarvan gebruik van een GMI toegestaan is en betrokkenen daarover niet hoeven te worden geïnformeerd.
3.	Het risico bestaat dat bij koppeling van data wordt afgeweken van het oorspronkelijke doel waarvoor persoonsgegevens in beginsel zijn verzameld.	In het kader van doelbinding is het van belang om vooraf vast te leggen onder welke omstandigheden informatie die is verkregen met het GMI kan worden gekoppeld aan informatie uit andere bronnen. In ogenschouw dient te worden genomen dat de koppeling plaatsvindt in overeenstemming met het oorspronkelijke doel waarvoor de gegevens in beginsel zijn verzameld.
4.	Voor het vaststellen van een normbeeld dient het GMI gedurende langere tijd te worden ingezet, waarbij het inherent is dat daarbij persoonsgegevens als bijvangst zullen worden verwerkt.	In het kader van minimale gegevensverwerking verdient het aanbeveling om een protocol op te stellen waarin is vastgesteld wanneer en welke signalen onder welke omstandigheden mogen worden geanalyseerd. Het normbeeld wordt dan niet automatisch vastgelegd door ongericht alle signalen op te vangen en uit te lezen, maar geschiedt weloverwogen en zorgvuldig door het stap voor stap te benaderen en te documenteren.
5.	Vooralsnog ontbreken specifieke bewaartermijnen voor eventuele persoonsgegevens die bij het gebruik van een GMI worden verwerkt.	Generieke bewaartermijnen vastleggen en een protocol opstellen waaruit blijkt op welke manier de vernietiging van de persoonsgegevens plaatsvindt. Indien

		het noodzakelijk is om persoonsgegevens langer te bewaren, dienen er aanknopingspunten te worden vastgelegd in het protocol onder welke omstandigheden langer bewaren geoorloofd is.
6.	Vooralsnog blijkt niet dat Defensie reeds heeft vastgesteld welke personen toegang kunnen krijgen tot de standalone laptop en de eventuele persoonsgegevens die daarop verwerkt zijn.	Het opstellen van een autorisatiematrix voor toegang tot de standalone laptop. Daarnaast moet worden zorggedragen voor een regelmatige update van het gehanteerde wachtwoord en eventueel voor tweefactor authenticatie voor zover dit nog niet uit het DBB volgt.
7.	De verwerking van persoonsgegevens bij deze activiteit is niet opgenomen in het verwerkingsregister van Defensie.	De verwerking van persoonsgegevens bij deze activiteit opnemen in het verwerkingsregister.

Activiteit 10A: Het Commando Zeestrijdkrachten voert digitale verkenningen uit door Defensie-gerelateerde onderwerpen of hashtags op het internet te onderzoeken.

Activiteit 10A Directie Operaties van het Korps Mariniers van het Commando Zeestrijdkrachten. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit Het Commando Zeestrijdkrachten verwerkt persoonsgegevens bij het uitvoeren van digitale verkenningen ten behoeve van eigen operationele informatie. Onder deze digitale verkenningen wordt het raadplegen van publicaties, sociale mediaberichten en andere bronnen verstaan die zichtbaar worden bij het zoeken op Defensie-gerelateerde onderwerpen of hashtags op het internet.		
Kwalificatie Deze activiteit is te kwalificeren als een activiteit van de krijgsmacht. Het uitvoeren van digitale verkenningen en het eventuele verwerken van persoonsgegevens daarbij valt aan te merken als gereedstellen.		
Conclusie Het Commando Zeestrijdkrachten (hierna: CZSK) beschikt niet over een bevoegdheid om persoonsgegevens te verwerken bij het uitvoeren van digitale verkenningen voorafgaand en tijdens gereedstelling. Voor zover er een bevoegdheid wordt gecreëerd, moet er nog extra aandacht worden besteed aan de informatieplicht, de bewaartermijnen en het verwerkingenregister. Daarom krijgt deze activiteit de kleur rood.		
Mogelijke knelpunten		Aanbevelingen
Juridisch		
1.	De bevoegdheid voor het verwerken van persoonsgegevens kan niet worden ontleend uit een wet in formele zin.	Het vaststellen van een wet in formele zin waaruit de bevoegdheid voor het verwerken van persoonsgegevens kan worden ontleend.
2.	Artikel 14 AVG bepaalt dat de betrokkene ook informatie moet ontvangen over: de contactgegevens van de Functionaris voor Gegevensbescherming (1b), de bewaartermijn van de	Het opnemen van een passage in de privacyverklaring voor medewerkers van Defensie, zodat de mariniers, voorafgaand aan de eventuele raadpleging van hun sociale mediaprofielen, op de hoogte zijn van de informatie uit artikel 14 AVG;

	persoonsgegevens (2a), de rechten van betrokkene (2c) en het klachtrecht (2e).	of een bepaling opnemen in de Militaire Ambtenarenwet 1931, waarin wordt bepaald dat mobiele apparaten en sociale mediaprofielen van medewerkers van Defensie kunnen worden gescreend.
3.	CZSK heeft geen bewaartermijnen vastgesteld voor de publicaties die worden opgeslagen en waar eventueel persoonsgegevens in voorkomen.	Het vaststellen van bewaartermijnen en deze bewaartermijnen vastleggen in de selectielijst van Defensie.
4.	De verwerking van persoonsgegevens is niet terug te vinden in het verwerkingenregister.	Het opnemen van de activiteit in het verwerkingenregister.

Activiteit 10B: Het Commando Zeestrijdkrachten slaat mogelijke relevante openbare nieuwsberichten op haar SharePoint.

Activiteit 10B Directie Operaties van het Korps Mariniers van het Commando Zeestrijdkrachten. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit Het Commando Zeestrijdkrachten (hierna: CZSK) verwerkt persoonsgegevens bij het uitvoeren van digitale verkenningen. Onder deze digitale verkenningen wordt het raadplegen van openbare nieuwberichten verstaan ter voorbereiding op een potentiële missie. Deze openbare nieuwsberichten worden, voor zover relevant voor de potentiële missie, opgeslagen op de SharePoint.		
Kwalificatie Deze activiteit is te kwalificeren als een activiteit van de krijgsmacht. Het raadplegen en opslaan van nieuwsberichten over mogelijke conflictgebieden in de wereld en het eventuele verwerken van persoonsgegevens daarbij valt aan te merken als gereedstellen.		
Conclusie Het Commando Zeestrijdkrachten beschikt niet over een bevoegdheid om persoonsgegevens te verwerken bij het raadplegen en opslaan van nieuwsberichten over conflictgebieden in de wereld. Voor zover er een bevoegdheid wordt gecreëerd, moet er nog extra aandacht worden besteed aan de informatieplicht, de bewaartermijnen en het verwerkingenregister. Daarom heeft deze activiteit de kleur rood.		
Mogelijke knelpunten		Aanbevelingen
Juridisch		
1.	De bevoegdheid voor het verwerken van persoonsgegevens kan niet worden ontleend uit een wet in formele zin.	Het vaststellen van een wet in formele zin waaruit de bevoegdheid voor het verwerken van persoonsgegevens kan worden ontleend.
2.	Betrokkenen kunnen op algemene wijze beter worden geïnformeerd over de verwerking van nieuwsberichten door CZSK.	Het toevoegen van een passage over de verwerking van nieuwsberichten in de privacyverklaring.

3.	CZSK heeft geen bewaartermijnen vastgesteld voor de nieuwsberichten die worden opgeslagen op de SharePoint.	Het vaststellen van bewaartermijnen en deze bewaartermijnen vastleggen in de selectielijst van Defensie.
4.	De verwerking van persoonsgegevens is niet terug te vinden in het verwerkingenregister.	Het opnemen van de activiteit in het verwerkingenregister.

Activiteit 11: De Surface and Assault Training Group van het Commando Zeestrijdkrachten stelt strandverkenningrapporten op.

Activiteit 11 Commando Zeestrijdkrachten – Surface Assault and Training Group. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit Surface and Assault Training Group (hierna: SATG) verzamelt data van stranden en verwerkt deze data in strandverkenningsrapporten. Deze rapporten bevatten informatie over waterdieptes en bodemgesteldheid, aangevuld met foto's om de situatie te duiden. Voor de validering van het rapport wordt de naam van de luitenant in het rapport verwerkt.		
Kwalificatie Deze activiteit valt onder de bedrijfsvoering van het Ministerie van Defensie. Het opstellen van strandverkenningsrapporten draagt immers bij aan de inzetbaarheid van krijgsmachtonderdelen.		
Conclusie SATG beschikt over een grondslag om de naam van de luitenant te verwerken in strandverkenningsrapporten. Wij zijn van mening dat SATG voor het verwerken van de naam van de luitenant een succesvol beroep kan doen op het gerechtvaardigd belang in de zin van artikel 6 lid 1 sub f AVG. Verder zijn er nog twee mogelijke knelpunten gesignaleerd. Daarom krijgt deze activiteit de kleur groen.		
Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	De strandverkenningsrapporten kennen geen bewaartermijnen en worden ook (nog) niet aangeboden ter archivering.	Het opstellen van bewaartermijnen voor strandverkenningsrapporten in de selectielijst van Defensie. Wanneer de bewaartermijn is verlopen, kan het strandverkenningsrapport – met doorhaling van de naam van de luitenant – worden gearchiveerd.
2.	De verwerking van de naam van de luitenant in een strandverkenningsrapport is nog niet expliciet opgenomen in het verwerkingenregister van Defensie.	Het opnemen van deze activiteit in het verwerkingenregister van Defensie.

Activiteit 12: Defensie Materieel Organisatie koopt en verkoopt defensiematerieel

Activiteit 12 Defensie Materieel Organisatie, afdeling Inkoop. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit De Defensie Materieel Organisatie (hierna: DMO) houdt zich bezig met aankoop, instandhouding en verkoop van defensiematerieel, IV en ICT. De afdeling Inkoop DMO legt ten behoeve van contractmanagement zakelijke gegevens van leveranciers en eindklanten vast in SAP M&F en Negometrix. Hierbij worden ook persoonsgegevens verwerkt.		
Kwalificatie De activiteiten van DMO vallen onder de bedrijfsvoering van het Ministerie van Defensie. Primair verwerkt DMO persoonsgegevens voor de uitvoering van een overeenkomst. Secundair verwerkt DMO persoonsgegevens voor de aankoop, instandhouding en verkoop van defensiematerieel. Een overheidsinstantie kan alleen een beroep doen op het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG), als er sprake is van een typisch bedrijfsmatige handeling. Wij zijn van mening dat de aankoop, instandhouding en verkoop van defensiematerieel als een typisch bedrijfsmatige handeling kwalificeert voor een overheidsinstantie als het Ministerie van Defensie. Deze activiteit kwalificeert daarom als interne bedrijfsvoering.		
Conclusie Er is een grondslag voor de verwerking van persoonsgegevens voor deze activiteit. Er zijn wel enkele mogelijke knelpunten gesignaleerd. Deze blokkeren de doorgang van deze activiteit echter niet. Daarom krijgt deze activiteit de kleur groen.		
Mogelijke knelpunten		Aanbevelingen
Juridisch		
1.	Bij de beoogde ingebruikname van SAP Ariba vindt mogelijk doorgifte van persoonsgegevens plaats buiten de EER.	Daar waar mogelijk, doorgifte van persoonsgegevens buiten de EER zoveel mogelijk voorkomen. Voor zover doorgifte buiten de EER zal plaatsvinden, dienen de vereisten voor doorgifte buiten de EER te worden nageleefd. Hieronder valt onder meer de actualisatie van de DPIA (SAP).
Organisatorisch		

2.	Mogelijk capaciteitsissue waardoor kennisvergaring over en inrichting van werkzaamheden conform de AVG mogelijk in mindere mate prioriteit krijgt. In dat geval kan dit leiden tot een verhoogd risico op privacy-/beveiligingsinbreuk.	Creëren van capaciteit en/of het creëren van prioriteit voor kennisvergaring en privacy bewustzijn.
----	---	---

Activiteit 13: Joint Informatievoorziening Commando ontwikkelt systemen voor Defensieonderdelen

Activiteit 13		
Joint Informatievoorziening Commando. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit		
Het Joint Informatievoorziening Commando (hierna: JIVC) houdt zich bezig met het ontwikkelen van systemen voor en het leveren van data aan klanten. Deze klanten zijn interne onderdelen binnen Defensie. Ook houdt JIVC zich bezig met experimenten op het gebied van IT (in de breedste zin van het woord). JIVC is vooral faciliterend en heeft geen tot weinig zicht op hoe klanten vervolgens omgaan met de verwerking van persoonsgegevens binnen die systemen. JIVC maakt bijvoorbeeld simulatieomgevingen of bepaalde systemen en voert data-analyses uit. Het bouwen van systemen vindt alleen intern plaats en is daarmee onderdeel van de (interne) bedrijfsvoering van Defensie.		
Kwalificatie		
Deze activiteit valt onder de bedrijfsvoering van het Ministerie van Defensie. Het ontwikkelen van de systemen door JIVC ziet namelijk toe op bedrijfsmatige handelingen en is puur gericht op de organisatie van Defensie. De grondslag voor het verwerken van persoonsgegevens ligt bij deze activiteit niet bij het JIVC. De interne klant van Defensie dient een grondslag te hebben voor de verwerking van persoonsgegevens in de systemen die JIVC ontwikkelt, bouwt en up-to-date houdt.		
Conclusie		
De activiteit kan doorgang vinden, maar er zijn wel enkele aanbevelingen gericht op bewustwording en naleving van de AVG. Vergroot de beschikbare capaciteit met betrekking tot privacy werkzaamheden binnen JIVC. Deze activiteit staat bovendien ook niet in het verwerkingsregister, wat volgens ons wel zou moeten. Afhankelijk of de wens bestaat dat JIVC meer inzicht in het gehele proces krijgt is het aan te bevelen om de procedures te herijken. Er zijn een aantal mogelijke knelpunten en aanbevelingen die zien op de naleving van de AVG. Deze aanbevelingen blokkeren de doorgang van deze activiteit echter niet. Daarom krijgt deze activiteit de kleur groen.		
Mogelijke knelpunten		Aanbevelingen
<i>Organisatorisch</i>		
1.	JIVC heeft te weinig inzicht of de klant aan de voor- en achterkant voldoende rekening houdt met de privacyregelgeving.	Richt procedures in waarbij aandacht wordt besteed aan rollen en verantwoordelijkheden tussen Defensieonderdelen en JIVC. Denk

		hierbij aan het opstellen van een werkhandleiding
2.	Er is een capaciteitstekort op het gebied van kennis van de geldende privacy (en aanverwante) wet- en regelgeving binnen JIVC.	Zorg voor voldoende kennis bij medewerkers over de AVG. Maar ook voor voldoende personeel dat zich bezighoudt met privacy gerelateerde vraagstukken, zoals het bijhouden van het verwerkingsregister en het uitvoeren van DPIA's. Zorg ook voor korte lijntjes tussen werknemers, de FG en de AVG-coördinator.
<i>Ethisch</i>		
3.	Door de politieke druk schiet personeel van JIVC in de kramp. Zo denkt personeel van JIVC dat ze bepaalde data-analyses niet uit kunnen voeren, terwijl er bij veel data-analyses geen persoonsgegevens worden verwerkt.	Door het vergroten van de kennis en bewustwording van de AVG weet personeel van JIVC wat de mogelijkheden zijn en wat wel en niet mag.

Activiteit 14A: Defensie Cyber Security Centrum beveiligt het interne IT-systeem van Defensie door middel van logging en monitoring

Activiteit 14A Joint IV Informatievoorziening Commando – Defensie Cyber Security Centrum. Deze activiteit vond plaats tijdens het onderzoek.	
Korte beschrijving activiteit De afdeling Defensie Cyber Security Centrum (hierna: DCSC) van Joint Informatievoorziening Commando (hierna: JIVC) houdt zich bezig met monitoring (actief) en logging (reactief). Het doel is om (eventuele) afwijkingen van het normale patroon zichtbaar te maken. Het systeem geeft deze afwijkingen aan doordat bepaalde regels en triggers zijn ingesteld. Vervolgens onderzoeken en analyseren gespecialiseerde analisten van DCSC deze afwijkingen, onder meer om false positives eruit te filteren. Bij noemenswaardige afwijkingen, stelt een analist een rapport op aan de hand van de bevindingen. Het monitoren en loggen vindt intern plaats en is daarmee onderdeel van de bedrijfsvoering. Het gaat hierbij om gepseudonimiseerde (bijvoorbeeld User ID) persoonsgegevens. Gepseudonimiseerde persoonsgegevens zijn niet anoniem in de zin van de Algemene Verordening Gegevensbescherming (hierna: AVG). Het doel van het verzamelen van deze persoonsgegevens is om defensiepersoneel dat (on)bewust mogelijk schadelijke handelingen verricht (eventueel) hierop aan te spreken en/of het cyberincident te volgen in het systeem.	
Kwalificatie Deze activiteit valt onder de bedrijfsvoering van het Ministerie van Defensie. Het monitoren en loggen van de systemen door DCSC is een typisch bedrijfsmatige handeling voor een overheidsinstantie, in dit geval van Defensie. Overheidsinstanties kunnen alleen een beroep doen op de grondslag artikel 6 lid 1 sub f van de AVG (gerechtvaardigd belang) als er sprake is van een typisch bedrijfsmatige handeling van een overheidsinstantie. Ingevolge overweging 49 AVG is de verwerking van persoonsgegevens, voor zover strikt noodzakelijk en evenredig met het oog op netwerk- en informatiebeveiliging, aan te merken als een gerechtvaardigd belang van een overheidsinstantie. Het is desalniettemin aan de verwerkingsverantwoordelijke om de afweging te maken of het verwerken van persoonsgegevens noodzakelijk en evenredig is en dat het gerechtvaardigd belang van Defensie prevaleert boven het belang van de betrokkene.	

Conclusie De activiteit kan in de huidige vorm doorgaan, maar er zijn mogelijk enkele knelpunten. Werk de (gerechtvaardigd) belangenafweging tussen het belang van de betrokkenen en de belangen van Defensie uit. De noodzakelijke belangenafweging ontbreekt volgens ons in de DPIA, daarom is niet met zekerheid te stellen of er sprake is van een gerechtvaardigd belang van Defensie om persoonsgegevens te verwerken, conform artikel 6 lid 1 sub f en overweging 49 AVG. Daarom krijgt deze activiteit de kleur oranje.		
Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	<p>De grondslag om deze activiteit uit te voeren is niet (duidelijk genoeg) gedefinieerd als taak van algemeen belang in de zin van artikel 6 lid 1 sub e AVG. Het juridisch kader is namelijk te algemeen om daar een specifieke taak uit te halen op grond waarvan DCSC persoonsgegevens mag verwerken.</p> <p>Daarom is deze activiteit ons inziens waarschijnlijk enkel op grond van het gerechtvaardigd belang uitvoerbaar. Er mist echter een vereiste belangenafweging tussen het belang van de betrokkenen en de belangen van Defensie.</p>	<p>Weeg de belangen van de betrokkenen af tegen de belangen van Defensie. Door deze belangenafweging te maken in de Data Protection Impact Assessment (hierna: DPIA) en het juridisch kader DCSC is de grondslag gerechtvaardigd belang conform artikel 6 lid 1 onder f AVG waarschijnlijk voldoende om activiteit 14A uit te voeren.</p>
2.	<p>DCSC ervaart privacy-issues met het verwerken van persoonsgegevens van Defensiepersoneel van privéapparatuur aangemeld op het Defensienetwerk. Op het netwerk monitort DCSC alle datastromen. De hoofdtak is het beschermen van het interne netwerk van Defensie. Af en toe detecteert DCSC 'gevaaren', zoals malware op privé-</p>	<p>Vergroot de privacy bewustwording van het Defensiepersoneel door middel van bijvoorbeeld phishingtests. Dit draagt bij aan de interne bescherming van het netwerk van Defensie, maar draagt er ook aan bij dat Defensiepersoneel zich beter weet te wapenen tegen eventuele phishingmails. Ons inziens wordt het mogelijke knelpunt hiermee (tenminste voor een gedeelte) gemitigeerd.</p>

	<p>apparatuur van Defensiepersoneel. De taak van DCSC is niet om deze apparaten te beschermen, maar DCSC heeft soms dus wel inzicht in mogelijke gevaren. DCSC mag in die gevallen niet optreden, terwijl dit wel makkelijk kan. Op het moment wordt in deze gevallen eerst toestemming gevraagd bij DJZ voordat actie wordt ondernomen.</p>	
<i>Ethisch</i>		
3.	<p>Het JIVC kan niet doorlopend op basis van MSOB of militaire bijstand ondersteuning verlenen. De belangen, bijvoorbeeld het beschermen van (oud) Defensiepersoneel (Veteraneninstituut) tegen cybercrime, zijn helder. De capaciteit en kennis zijn eveneens aanwezig. Het is op dit moment niet mogelijk om extern deze capaciteit te leveren.</p>	<p>Beoordeel aan de voorkant of het wenselijk is dat JIVC (of een ander defensieonderdeel, bijvoorbeeld DCC) zich bezighouden met deze of soortgelijke activiteiten.</p>

Activiteit 14B

<zie vertrouwelijke bijlage>

Activiteit 15:

<zie vertrouwelijke bijlage>

Activiteit 16:

<zie vertrouwelijke bijlage>

Activiteit 17:

<zie vertrouwelijke bijlage>

Activiteit 18: Dienstcentrum Personeelslogistiek houdt zich bezig met de arbeidsmarktcommunicatie

Activiteit 18 Dienstcentrum Personeelslogistiek. Deze activiteit vond plaats tijdens het onderzoek.	
Korte beschrijving activiteit Het Dienstcentrum Personeelslogistiek (hierna: DCPL) werft, selecteert en keurt nieuw militair- en burgerpersoneel voor Defensie. Jaarlijks worden ongeveer 4000-5000 mensen aangesteld. Aangezien slechts een klein deel van alle personen die zich aanmelden wordt aangesteld, moet er door middel van campagnes een groot publiek worden bereikt. Het aanstellen van nieuw personeel gaat over verschillende schijven (werven, selecteren en keuren). Deze activiteit ziet alleen toe op het onderdeel 'arbeidsmarktcommunicatie'. Werven en Selecteren (hierna: WenS) omvat alle werving en selectie activiteiten, beginnend bij het opstellen van een wervingsstrategie en eindigend met de selectie van een kandidaat, inclusief vastlegging en bevestiging van arbeidsvoorwaarden. Het proces stopt bij 'klaar voor aanstelling'. Arbeidsmarktcommunicatie is op zichzelf gezien een onderdeel van werving en omvat arbeidsmarktcampagnes, sociale media en de website (www.werkenbij...).	
Kwalificatie Activiteiten die samenhangen met arbeidsmarktcommunicatie zien toe op de bedrijfsvoering van Defensie. De activiteit is van ondersteunende aard, maar ziet niet op inzet/gereedstellen van de krijgsmacht.	
Conclusie Er is een grondslag voor de verwerking van persoonsgegevens voor deze activiteit. Er zijn wel enkele mogelijke knelpunten gesignaleerd. Deze blokkeren de doorgang van deze activiteit echter niet. Daarom krijgt deze activiteit de kleur groen.	
Mogelijke knelpunten	Aanbevelingen
Juridisch	
1 Het is ons opgevallen dat er geen ondubbelzinnige, actieve handeling vooraf gaat aan het stellen van een vraag via https://werkenbijdefensie.nl/contact/stuur-een-mail . Hierdoor is het voor de betrokkene mogelijk	Informeer de betrokkene over de verwerking van zijn persoonsgegevens. Het vereisen van een actieve handeling van de betrokkene kan hiervoor een invulling zijn, bijvoorbeeld het aanvinken van een akkoordverklaring. Voor een voorbeeld verwijzen wij naar:


	onvoldoende duidelijk welke persoonsgegevens voor welk doel worden verwerkt.	https://www.rijksoverheid.nl/contact/informatie-rijksoverheid/e-mail-sturen
2	De privacyverklaring op de website werkenbijdefensie.nl/privacyverklaring schiet op enkele vlakken tekort: Verwerking van persoonsgegevens in Coosto als derde partij wordt niet genoemd; Er is niets opgenomen over geautomatiseerde besluitvorming, terwijl dit wel wordt toegepast.	De privacyverklaring is voor het laatst gewijzigd op 1 mei 2020. Het is raadzaam om een proces in te richten waarbij bijvoorbeeld jaarlijks de privacyverklaring wordt bekeken en zo nodig geüpdatet. Neem in ieder geval Coosto en geautomatiseerde besluitvorming op in de volgende versie.
3	Het is vrijwel onvermijdelijk om bij arbeidscommunicatie geen gebruik te maken van de big tech firma's voor effectieve campagnevoering. Probleem hierbij is dat het niet mogelijk is om individuele afspraken te maken met deze partijen. Ook worden hierbij persoonsgegevens verwerkt buiten de Europese Economische Ruimte (hierna: EER).	Betrokkenen die gebruikmaken van sociale media en WhatsApp zijn reeds zelfstandig akkoord gegaan met de verwerking van persoonsgegevens buiten de EER. Het is wel aan te raden om dit in het kader van transparantie ook in de privacyverklaring van werkenbijdefensie.nl op te nemen. Geef daarbij ook een toelichting dat er sprake is van internationale doorgifte van persoonsgegevens en geef aan wat daarvan de gevolgen zijn. Het is verstandig om een heldere standaardtekst op te stellen om te versturen zodra een betrokkene contact zoekt via WhatsApp. Neem deze tekst ook op in de privacyverklaring van Contact - WerkenbijDefensie.nl .

Activiteit 19: Dienstcentrum Personeelslogistiek voert arbeidsmarktanalyses uit

Activiteit 19		
Dienstcentrum Personeelslogistiek. Deze activiteit vond plaats tijdens het onderzoek.		
Korte beschrijving activiteit		
Bureau accountmanagement, onderdeel van het Dienstcentrum Personeelslogistiek (hierna: DCPL) voert arbeidsmarktanalyses uit. De arbeidsmarktanalist gebruikt (geaggregeerde) data uit verschillende bronnen. Het doel van deze analyses is het verkrijgen van een duidelijk beeld van de ontwikkelingen op de arbeidsmarkt. Door de knelpunten van de arbeidsmarkt te analyseren constateert de arbeidsmarktanalist waar de krapte in de markt zit. Hier kan DCPL dan tijdig op reageren. Volgens de respondenten is de aangeleverde geaggregeerde informatie aan de voorkant geanonimiseerd en door Defensie niet te herleiden naar natuurlijke personen.		
Kwalificatie		
Activiteiten die samenhangen met arbeidsmarktanalyse zien toe op de bedrijfsvoering van Defensie. De activiteit is van ondersteunende aard, maar ziet niet op inzet/gereedstellen van de krijgsmacht. Er is bij deze activiteit geen sprake van een publieke taak. Wel is de activiteit waarschijnlijk aan te merken als een typisch bedrijfsmatige handeling. Om die reden is de grondslag om deze activiteit uit te voeren waarschijnlijk het gerechtvaardigd belang conform artikel 6 lid 1 sub f van de Algemene verordening gegevensbescherming (hierna: AVG). Hiervoor moet nog wel de benodigde belangenafweging tussen het belang van Defensie en het belang van de betrokkene worden uitgevoerd.		
Conclusie		
Op dit moment wordt bij deze activiteit niet voldaan aan de beginselen van artikel 5 AVG. Dit komt omdat medewerkers van DCPL niet bewust zijn van enige verwerking van persoonsgegevens. Het gaat weliswaar om indirect herleidbare persoonsgegevens, maar ook hierop is de AVG van toepassing. Het advies is om deze beginselen alsnog tegen het licht te houden bij deze activiteit. Als daarbij invulling wordt gegeven aan de beginselen kan deze activiteit volgens ons mogelijk alsnog doorgang vinden. De activiteit kan waarschijnlijk op korte termijn doorgang vinden, mits wordt voldaan aan de beginselen van artikel 5 AVG. Daarom krijgt deze activiteit de kleur oranje.		
Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Bij deze activiteit wordt momenteel geen rekening	Geef invulling aan de beginselen van artikel 5 AVG, aangezien er indirect

	<p>gehouden met de beginselen van artikel 5 AVG. Medewerkers zijn zich niet bewust dat er (indirect herleidbare) persoonsgegevens worden verwerkt en de AVG is dus wel van toepassing is op deze activiteit.</p>	<p>herleidbare persoonsgegevens worden verwerkt.</p> <p>Bij de invulling van de rechtmatigheid kan daarbij mogelijk aansluiting worden gezocht bij de grondslag gerechtvaardigd belang.</p>
--	--	---

Activiteit 20 t/m 22: Geografische Informatie

Activiteit 20, 21 en 22		
Geo-informatie diensten. Deze activiteiten vonden plaats tijdens het onderzoek.		
Korte beschrijving activiteit		
Geografische informatie (hierna: GI) is essentieel voor Defensie en het informatie gestuurd optreden (hierna: IGO). In alle domeinen en functies van militair optreden is geografische informatie noodzakelijk om te analyseren, te plannen en om situational awareness te krijgen. Bij Defensie zijn hiervoor drie GI-eenheden verantwoordelijk: 1. De Dienst Geografie (hierna: DGeo) - activiteit 20 2. De Dienst der Hydrografie (hierna: DHydro) - activiteit 21; 3. Joint Meteo Groep (hierna: JMG) - activiteit 22. Bij deze activiteiten worden geen persoonsgegevens verwerkt.		
Kwalificatie		
Deze activiteiten zijn te kwalificeren als (ondersteunen bij) inzet en gereedstelling. Er is geen sprake van interne bedrijfsvoering.		
Conclusie		
Bij deze activiteiten worden geen persoonsgegevens verwerkt. Daarom zijn er ook geen knelpunten die betrekking hebben op de Algemene verordening gegevensbescherming (hierna: AVG). De activiteiten kunnen op de huidige manier doorgaan. Daarom krijgt deze activiteit de kleur groen.		
Mogelijke knelpunten		Aanbevelingen
Organisatorisch		
1.	Volgens de respondent zit DGeo te diep 'weggestopt' in de organisatie. Het is van belang dat Defensieonderdelen tijdig informeren bij DGeo als zij bijvoorbeeld nieuw materiaal aankopen. Het moet namelijk wel mogelijk zijn om de GI (zoals kaarten) digitaal aanwezig te hebben in bijvoorbeeld vliegtuigen. Als het vliegtuig het systeem waarin Defensie werkt niet ondersteunt, dan levert dit achteraf extra kosten op.	Bepaal de positie van de GI-eenheden binnen de Defensieorganisatie. Ook kan het goed zijn om op centraal niveau deskundigen te positioneren. Hierdoor is een verbeteringsslag te maken op het gebied van bewustwording over het gebruik van de juiste geo data en standaarden.

5 Wettelijk toetsingskader

5.1 Inleiding

De Algemene verordening gegevensbescherming (hierna: AVG) en de Uitvoeringswet algemene verordening gegevensbescherming (hierna: UAVG) bevatten regels over de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens.²⁶ Een recht dat des te belangrijker is geworden in de huidige informatiemaatschappij, waarbinnen de verwerking van persoonsgegevens onvermijdelijk is.

Het Ministerie van Defensie (hierna: Defensie) wenst ook een rol van betekenis te spelen in deze informatiemaatschappij. De informatiemaatschappij kan diverse Defensieonderdelen (hierna: DO'en) namelijk van nuttige en bruikbare informatie voorzien, wat enerzijds kan bijdragen aan de taakvervulling van de onderliggende krijgsmachtonderdelen en anderzijds aan de digitale uitvoering van bestaande activiteiten door andere DO'en. Alvorens Defensie haar activiteiten kan verrichten in de informatiemaatschappij, is het van belang inzichtelijk te hebben in hoeverre Defensie deze activiteiten mag uitvoeren op basis van de geldende wet- en regelgeving.

77

5.2 Opzet

In dit hoofdstuk wordt het toetsingskader artikelsgewijs uiteengezet aan de hand van het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM), de Grondwet (hierna: Gw) en de AVG. Allereerst komen artikel 8 EVRM en artikel 10 Gw aan bod. Vervolgens wordt aandacht besteed aan de AVG met allereerst het materiële toepassingsbereik (artikel 2 AVG en artikel 3 UAVG), gevolgd door het territoriale toepassingsbereik (artikel 3 AVG). Daarna worden de beginselen inzake verwerking van persoonsgegevens uiteengezet (artikel 5 en 6 AVG). Gelet op het feit dat de AVG vereist dat de verwerkingsverantwoordelijke een administratie bijhoudt van haar gegevensverwerking, komt de verantwoordingsplicht (artikel 5 lid 2 AVG) ook aan bod.

²⁶ Zie artikel 1 lid 1 AVG.

5.3 Europees Verdrag voor de Rechten van de Mens

De Nederlandse vertaling van artikel 8 EVRM luidt als volgt:

1. *“Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.*
2. *Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen.”*

Hoewel de bescherming van persoonsgegevens niet wordt genoemd in artikel 8 lid 1 EVRM, is door het Europees Hof voor de Rechten van de Mens (hierna: EHRM) erkend dat het artikel ook de bescherming van persoonsgegevens omvat.²⁷

De AVG is een uitwerking van artikel 8 Handvest van de grondrechten van de Europese Unie (hierna: Handvest) en artikel 16 Verdrag betreffende de werking van de Europese Unie (hierna: VWEU). Als onderdeel van de bescherming van het privéleven is ook artikel 8 EVRM en artikel 17 Internationaal Verdrag inzake burgerrechten en politieke rechten (hierna: IVBPR) relevant. Op grond van artikel 16 VWEU heeft eenieder het recht op bescherming van zijn of haar persoonsgegevens.²⁸

78

5.4 Grondwet

Artikel 10 Gw bepaalt het volgende:

1. *“Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.*
2. *De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.*
3. *De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.”*

²⁷ H.R. Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, artikel 8 EVRM, aantekening 1.

²⁸ Zwenne/Zwenne & Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, inleidende opmerkingen aantekening 2. Grondrechtelijke aspecten.

Het recht op eerbiediging van de persoonlijke levenssfeer zoals neergelegd in de Gw is een direct werkend recht dat een verplichting inhoudt voor de overheid om zich van optreden te onthouden, tenzij een wet in formele zin daartoe een grondslag biedt. Een nadere omlijning van het begrip 'persoonlijke levenssfeer' moet gezocht worden in de rechtspraak, waarbij de jurisprudentie van het EHRM over artikel 8 EVRM een leidende rol speelt.²⁹

Bij de eerbiediging van de persoonlijke levenssfeer neemt de bescherming van persoonsgegevens een speciale plaats in.³⁰ Door allerlei gegevens omtrent personen te registreren, deze in verband met elkaar te brengen en vervolgens bij het nemen van voor de persoon belangrijke beslissingen van die gegevens gebruik te maken, kan de privacy worden aangetast. Doorslaggevend daarbij is niet dat al die gegevens intieme informatie bevatten. De privacy-aantasting kan hierin gelegen zijn, dat over de individuele burger met al zijn hoedanigheden, gedragingen en andere kenmerken, welke zijn persoon en zijn leven vormen, op allerlei plaatsen gegevens worden vastgelegd en dat dit geheel van gegevens een steeds grotere invloed gaat krijgen op voor hem belangrijke zaken, zoals het verkrijgen van huisvesting, de opbouw van een loopbaan, het verwerven van geldleningen, etc. Aldus kan een situatie ontstaan waarin de burger onvoldoende ruimte overhoudt om zijn eigen leven te leiden met zo weinig mogelijk inmenging van buitenaf.³¹

79

5.5 Materieel toepassingsbereik AVG

Artikel 2 lid 1 AVG bepaalt dat de AVG van toepassing is op de geheel of gedeeltelijk geautomatiseerde verwerking, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Op basis van deze wetsbepaling wordt beoordeeld of de AVG op de verwerking van persoonsgegevens van toepassing is.

²⁹ H.R. Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, art. 10 Grondwet, aantekeningen 1 en 2.

³⁰ Het begrip privéleven (ook wel persoonlijke levenssfeer of privacy genoemd) wordt door het EHRM ruim opgevat. Het omvat de fysiologische en psychologische integriteit van een individu en behelst onder meer het recht op identiteit en persoonlijke ontwikkeling, het recht om relaties op te bouwen met andere mensen en met de buitenwereld. Er is een gebied van interactie van een persoon met anderen, zelfs in het publieke domein, die onder de reikwijdte van het begrip 'privéleven' valt. Het privéleven is derhalve niet beperkt tot de 'inner circle' van de intieme privésfeer van een persoon, maar kan zich ook uitstrekken tot de werkvloer of het publieke domein. H.R. Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, commentaar op art. 8 EVRM, aantekeningen 1 en 2.

³¹ H.R. Kranenborg, in: *T&C Privacy- en gegevensbeschermingsrecht*, artikel 10 Grondwet, aantekening 3.

Persoonsgegevens

Artikel 4 onder 1) geeft de definitie van het begrip 'persoonsgegevens'. Onder persoonsgegevens wordt het volgende verstaan: "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 identifier zoals een naam, een identificatienummer, locatiegegevens, een online identifier of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon."

Onder deze definitie vallen onder meer de volgende categorieën persoonsgegevens: adres, biometrische gegevens, Burgerservicenummer, e-mailadres, feiten en waarderingsen over gedragingen, opmerkingen en/of eigenschappen, financiële gegevens, foto's, video's en/of spraakopnames, functie, geboortedatum, gegevens van strafrechtelijke aard, geloof, geslacht, gezondheidsgegevens, inloggegevens, IP-adres/MAC-adres, kenteken (voertuig), lidmaatschap vakbond, locatiegegevens, naam, politieke voorkeur, ras en etniciteit, seksuele voorkeur en telefoonnummer.

Opmerking verdient dat Defensie beschikt over uiteenlopende mogelijkheden en middelen om personen mee te identificeren. Hierdoor is Defensie ook in staat om personen (indirect) te identificeren aan de hand van bijvoorbeeld radio roepnaam en ATIS, Europa-nummer, IMO-nummer, MMSI, telefaxnummer, scheepsnaam, uiterlijke kenmerken van een schip en metadata.³² Gelet daarop is het bij dit onderzoek van belang om bij de beoordeling van de activiteiten verder te kijken dan de algemeen bekende categorieën persoonsgegevens, zoals genoemd in de vorige alinea.

80

Uitzonderingen

Artikel 2 lid 2 sub a en b AVG bepaalt dat de AVG niet van toepassing is op de verwerking van persoonsgegevens (a) in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen en (b) door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, Verdrag betreffende de Europese Unie (hierna: VEU) vallen. Titel V, hoofdstuk 2, VEU heeft betrekking op extern optreden en gemeenschappelijk (Europees) buitenlands en veiligheidsbeleid.

De schakelbepaling in artikel 3 lid 1 jo lid 2 UAVG bepaalt echter dat de AVG wel van toepassing is op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen.

³² Zie Verwerking M8107 uit het AVG-register Kustwacht Centrum (KWC).

De Memorie van Toelichting op de UAVG zegt over de werkingssfeer van het Unierecht dat alleen gegevensverwerkingen die in hun geheel zijn uitgezonderd van de werking van het Europees recht buiten de materiële werkingssfeer van de verordening vallen. De Nederlandse regering gaat er voornamelijk van uit dat dit alleen geldt voor verwerkingen in het kader van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: WIV 2017) en verwerkingen door de krijgsmacht ten behoeve van de uitvoering van haar taken, bedoeld in artikel 97 van de Grondwet (hierna: Gw) (de verdediging en bescherming van de belangen van het Koninkrijk en de handhaving en bevordering van de internationale rechtsorde).³³

Op de verwerking van persoonsgegevens in het kader van de taken van de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD) is bij Defensie niet de AVG, maar de WIV 2017 van toepassing.

Artikel 2 lid 2 sub d AVG bepaalt dat de AVG niet van toepassing is op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de opsporing en vervolging van strafbare feiten. Dit betreft bij Defensie de verwerkingen die door de Koninklijke Marechaussee (hierna: KMar) worden uitgevoerd in verband met de in de Politiewet opgedragen rechtshandavingstaken en openbare ordetaken en de militaire bijstand aan bijvoorbeeld de politie door andere onderdelen van de krijgsmacht. Op deze verwerking van persoonsgegevens is in plaats van de AVG de Richtlijn gegevensbescherming politie en justitie³⁴ en de daarop gebaseerde Wet Politiegegevens (hierna: WPG) van toepassing.

Om te voldoen aan de regelingsplicht van artikel 10 Gw en om te voorkomen dat op dergelijke verwerkingen door de krijgsmacht ten behoeve van de uitvoering van haar taken, bedoeld in artikel 97 van de Gw in het geheel geen regels omtrent de bescherming van de persoonlijke levenssfeer van toepassing zouden zijn, worden de UAVG en de AVG op deze verwerkingen respectievelijk van toepassing en van overeenkomstige toepassing verklaard (artikel 3 UAVG).³⁵

Ook in het geval van inzet of het ter beschikking stellen van de krijgsmacht dienen waar mogelijk de algemene beginselen voor de verwerking van persoonsgegevens in acht te worden genomen. Er moet evenwel een mogelijkheid zijn om af te wijken, omdat bij inzet in internationale militaire operaties niet altijd kan worden vereist dat alle bepalingen onverkort worden

³³ Zie Kamerstukken 34 851, vergaderjaar 2017-2018 (p. 90).

³⁴ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende gegevensbescherming politie en justitie (PbEU 2016, L 119/89).

³⁵ Zie Kamerstukken 34 851, vergaderjaar 2017-2018 (p. 91).

toegepast. De omstandigheden waarin de krijgsmacht soms moet functioneren, laten dat niet altijd toe. Hierom is het wenselijk om de Minister van Defensie de bevoegdheid te geven om hierop een uitzondering te maken als er sprake is van daadwerkelijke operationele inzet van de krijgsmacht.³⁶

Daarom bepaalt de regering in artikel 3 lid 3 UAVG dat de AVG, de UAVG en de daarop berustende bepalingen enkel niet (volledig) van toepassing zijn op de verwerking van persoonsgegevens door de krijgsmacht, voor zover Onze Minister van Defensie daartoe beslist met het oog op inzet of het ter beschikking stellen van de krijgsmacht ter uitvoering van de in artikel 97 Gw omschreven taken; en op de verwerking van persoonsgegevens voor zover daarop de WIV 2017 van toepassing is.³⁷

Van operationele inzet van de krijgsmacht is volgens de Memorie van Toelichting op artikel 97 Gw sprake wanneer uitvoering wordt gegeven aan één van onderstaande taken:

- a. de verdediging van het Koninkrijk, met inbegrip van de bondgenootschappelijke verdediging, zoals in het kader van de NAVO en de (medio 2011 opgeheven) West-Europese Unie;
- b. de bescherming van de (andere) belangen van het Koninkrijk. Te denken valt bijvoorbeeld aan bijstand aan de politie ter handhaving van de openbare orde, voor de strafrechtelijke handhaving van de rechtsorde of voor het verrichten van taken ten dienste van justitie (art. 58 Politiewet 2012), de hulpverlening aan burgers in nood en de bijstandsverlening bij rampenbestrijding;
- c. De handhaving en de bevordering van de internationale rechtsorde. De term 'handhaving' is ontleend aan artikel 39 VN-Handvest en ziet op militair optreden vanwege schendingen van de internationale rechtsorde. De term 'bevordering' sluit aan bij artikel 90 Gw en ziet op alle maatregelen die aan de internationale rechtsorde dienstig zijn. Deze maatregelen mogen niet in strijd zijn met het Handvest van de Verenigde Naties. Onder de bevordering van de internationale rechtsorde valt ook de verlening van humanitaire hulp in het buitenland zonder dat er sprake is van een gewapend conflict. Ter zake van de besluitvorming van de regering en het overleg met het parlement over de inzet of terbeschikkingstelling van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde, met inbegrip van humanitaire hulpverlening in geval van een gewapend conflict, heeft het kabinet een 'Toetsingskader' vastgesteld, dat laatstelijk in 2014 is herzien.³⁸

³⁶ Zie Kamerstukken 34 851, vergaderjaar 2017-2018 (p. 91).

³⁷ Zie artikel 3 lid 3 UAVG.

³⁸ MvT, Kamerstukken II 1996/97, 25367 (R 1593), 3, p. 3-4.

Op basis van artikel 3 lid 3 onder a van de UAVG heeft de Staatssecretaris van Defensie enkele uitzonderingen geformuleerd die zijn neergelegd in de Regeling Gegevensbescherming Militaire Operaties (hierna: RGMO). Artikel 1 lid 1 RGMO bepaalt dat bepaalde delen van de AVG en UAVG niet van toepassing zijn op de verwerking van persoonsgegevens ter uitvoering van de in artikel 97 Gw omschreven taken voor zover dat noodzakelijk is voor de uitvoering van het mandaat en de bescherming van de troepenmacht. Gelet op het feit dat Defensie reeds bekend is met haar bevoegdheden ten tijde van inzet, merken wij op dat dit onderzoek zich uitsluitend richt op activiteiten van krijgsmachtonderdelen buiten inzet en DO'en die niet tot de krijgsmacht behoren.

5.6 Territoriaal toepassingsbereik AVG

Artikel 3 lid 1 AVG bepaalt dat de AVG van toepassing is op de verwerking van persoonsgegevens in het kader van de activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Unie, ongeacht of de verwerking in de Unie al dan niet plaatsvindt.

Defensie verwerkt persoonsgegevens onder verantwoordelijkheid van de Minister van Defensie. Inzet van Defensie ten behoeve van militaire bijstand conform de Wet veiligheidsregio's, de Politiewet 2012 of Militaire steunverlening in het openbaar belang (hierna: MSOB) of vindt plaats onder verantwoordelijkheid van het civiele gezag. Voor zover daar in dit rapport sprake van is, wordt dat bij de uitwerking van de activiteit expliciet aangegeven.

83

5.7 De beginselen van artikel 5 AVG

Een verwerking van persoonsgegevens dient volgens artikel 5 AVG in overeenstemming te zijn met een aantal beginselen. Deze beginselen worden hier achtereenvolgens behandeld.

5.7.1 Rechtmatigheid, behoorlijkheid en transparantie

Het Unierecht (artikel 5 lid 1 sub a AVG) en het recht van de Raad van Europa inzake gegevensbescherming eisen dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is³⁹. Om persoonsgegevens rechtmatig te verwerken is

³⁹ Handbook on European data protection law (2018 edition) H4.1.1.; Handboek Europese gegevensbeschermings-wetgeving. (europa.eu)

toestemming van de betrokkene vereist of een andere legitieme reden.⁴⁰ Artikel 6 lid 1 AVG biedt in dat kader zes grondslagen op basis waarvan een verwerking van persoonsgegevens rechtmatig is.⁴¹ Het beginsel van rechtmatigheid en in het verlengde daarvan de grondslagen nader uitgewerkt in paragraaf 5.8.

Onder behoorlijkheid wordt verstaan dat betrokkenen op behoorlijke wijze op de hoogte worden gebracht van de (aanstaande) gegevensverwerking. Artikel 12 lid 1 AVG vereist dat de informatie over de gegevensverwerking in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in duidelijke en eenvoudige taal wordt verstrekt.

Met transparantie wordt bedoeld dat de verwerkingsverantwoordelijk duidelijke informatie verschaft over onder andere het doel van de verwerking (artikel 13 lid 1 jo lid 2 AVG en de Guidelines under transparency⁴²). De AVG bepaalt welke informatie aan de betrokkene moet worden verstrekt en maakt hierbij een onderscheid in informatieverstrekking, afhankelijk van of de betreffende persoonsgegevens van de betrokkene zelf zijn verkregen, of van een andere bron.⁴³

84

5.7.2 Doelbinding

Artikel 5 lid 1 sub b AVG bepaalt dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden moeten worden verzameld en vervolgens niet verder op een met die doeleinden onverenigbare wijze mogen worden verwerkt; de verdere verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden wordt overeenkomstig artikel 89, lid 1, niet als onverenigbaar met de oorspronkelijke doeleinden beschouwd.

Uit deze omschrijving blijkt dat de doelen helder moeten zijn op het moment dat de persoonsgegevens worden verzameld en expliciet en gerechtvaardigd moeten zijn.⁴⁴

⁴⁰ Conform artikel 8 lid 2 Handvest, artikel 5 lid 2 Gemoderniseerd Verdrag 108 en artikel 6 t/m 9 AVG. Ons onderzoek richt zich met betrekking tot de uitwerking van de rechtmatigheid van de verwerking in deze paragraaf tot de AVG.

⁴¹ Voor het verwerken van gewone en gevoelige persoonsgegevens is het voldoende om een grondslag te hebben op basis van artikel 6 lid 1 AVG. Voor het verwerken van bijzondere persoonsgegevens geldt er een verwerkingsverbod tenzij er een uitzondering van toepassing is. Dit betekent dat voor het verwerken van bijzondere persoonsgegevens naast een grondslag op basis van artikel 6 lid 1 AVG ook een uitzondering op grond van artikel 9 lid 2 AVG van toepassing moet zijn.

⁴² Guideline van de artikel 29 Werkgroep van 11 april 2018, nu de European Data Protection Board.

⁴³ Vgl. artikel 13 en 14 AVG. Zie ook overweging 50 AVG.

⁴⁴ Zie overweging 39 van de AVG.

Wanneer persoonsgegevens voor een bepaald doel zijn verzameld, dan mogen deze alleen verder worden verwerkt, wanneer dat doel verenigbaar is met het primaire doel. Of dat het geval is, wordt bepaald aan de hand van een aantal factoren:

- a. het verband tussen de doeleinden waarvoor de gegevens zijn verzameld en de doeleinden van de verdere verwerking;
- b. het kader waarin de persoonsgegevens zijn verzameld en dan met name de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke (ook wel: de wijze van verkrijging en de verwachting van de betrokkene);
- c. de aard van de gegevens;
- d. de mogelijke gevolgen van de voorgenomen verdere verwerking voor betrokkenen; en
- e. het bestaan van passende waarborgen, zoals pseudonimisering.

Indien op basis van deze vereisten wordt geoordeeld dat de verdere verwerking onverenigbaar is met het primaire doel, dan is de verdere verwerking alleen toegestaan, indien betrokkene daarvoor toestemming heeft gegeven of indien de verdere verwerking berust op een Europese of nationale wettelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van een in artikel 23 lid 1 AVG bedoeld doeleinde (nationale veiligheid, landsverdediging en openbare veiligheid). Daarnaast is verdere verwerking ook toegestaan, indien de verdere verwerking plaatsvindt met het oog op wetenschappelijk onderzoek.⁴⁵

5.7.3 Minimale gegevensverwerking

Artikel 5 lid 1 sub c AVG bepaalt dat persoonsgegevens toereikend, ter zake dienend en beperkt moeten zijn tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt.

Met minimale gegevensverwerking of dataminimalisatie wordt bedoeld dat alleen die persoonsgegevens worden gebruikt die noodzakelijk zijn om het welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doel te bereiken. Alleen die persoonsgegevens die noodzakelijk zijn voor de doeleinden waarvoor ze zijn verkregen mogen worden verwerkt.

⁴⁵ Zie artikel 6 lid 4 AVG.

5.7.4 Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd; alle redelijke maatregelen moeten worden genomen om de persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

De verwerkingsverantwoordelijke kan niet (zonder meer) uitgaan van de juistheid van de gegevens uit de verschillende (openbare) bronnen en is zelf verantwoordelijk voor de controle en het waarborgen van de juistheid, integriteit en actualiteit van de verwerkte gegevens. De verwerkingsverantwoordelijke moet maatregelen treffen om de juistheid van de persoonsgegevens te waarborgen. Zo moet de verwerkingsverantwoordelijke persoonsgegevens die onjuist zijn aanpassen of verwijderen.

5.7.5 Opslagbeperking

Artikel 5 lid 1 sub e AVG bepaalt dat persoonsgegevens moeten worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan voor de doeleinden waarvoor de persoonsgegevens worden verwerkt noodzakelijk is; persoonsgegevens mogen voor langere perioden worden opgeslagen voor zover de persoonsgegevens louter met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden worden verwerkt overeenkomstig artikel 89, lid 1, mits de bij deze verordening vereiste passende technische en organisatorische maatregelen worden getroffen om de rechten en vrijheden van de betrokkene te beschermen.

86

Het beginsel van opslagbeperking brengt in de praktijk met zich mee dat de verwerkingsverantwoordelijke voor elke verwerking een bewaartermijn moet vaststellen.

5.7.6 Integriteit en vertrouwelijkheid

Artikel 5 lid 1 sub f AVG bepaalt dat persoonsgegevens door het nemen van passende technische of organisatorische maatregelen op een dusdanige manier moeten worden verwerkt, dat een passende beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Artikel 32 AVG vereist dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen neemt ter beveiliging van de persoonsgegevens. Met organisatorische maatregelen worden maatregelen

bedoeld die betrekking hebben op de inrichting en werking van de organisatie en haar medewerkers. Hieronder wordt onder meer de fysieke beveiliging van (technische) apparaten en ruimtes, het autoriseren van daartoe bevoegde personen, het onderwerpen aan een screening van nieuw personeel en het tekenen van een geheimhoudingsverklaring door betrokken personen verstaan.

In dit onderzoek zijn wij ervan uitgegaan dat de verwerking van persoonsgegevens is onderworpen aan geavanceerde technische en organisatorische maatregelen op grond van het Defensiebeveiligingsbeleid (hierna: DBB). De beoordeling van de technische en organisatorische maatregelen is in dit onderzoek dan ook buiten beschouwing gelaten.

5.7.7 Verantwoordingsplicht

Artikel 5 lid 2 AVG bepaalt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen uit artikel 5 lid 1 AVG en de naleving daarvan kan aantonen. Dit wordt aangeduid als de verantwoordingsplicht.

De verantwoordingsplicht brengt niet alleen met zich mee dat in de praktijk aan voorwaarden moet worden voldaan, maar dat dit ook moet worden vastgelegd. Een besluit over de verwerking van persoonsgegevens moet op een later tijdstip reproduceerbaar zijn aan de hand van de vastlegging van de besluitvorming. Een organisatie moet aantoonbaar gedocumenteerd compliant zijn. De verwerkingsverantwoordelijke kan op verschillende manieren aan de verantwoordingsplicht voldoen:

Verwerkingsregister

Artikel 30 lid 1 AVG bepaalt dat elke verwerkingsverantwoordelijke en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke een register bijhoudt van de verwerkingsactiviteiten die onder hun verantwoordelijkheid plaatsvinden. Dat register moet in ieder geval deze informatie bevatten:

- a. de naam en de contactgegevens van de verwerkingsverantwoordelijke en eventuele gezamenlijke verwerkingsverantwoordelijken, en, in voorkomend geval, van de vertegenwoordiger van de verwerkingsverantwoordelijke en van de functionaris voor gegevensbescherming;
- b. de verwerkingsdoeleinden;
- c. een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;

- d. de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, onder meer ontvangers in derde landen of internationale organisaties;
- e. indien van toepassing, doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of die internationale organisatie en, in geval van de in artikel 49 lid 1, tweede alinea, bedoelde doorgiften, de documenten inzake de passende waarborgen;
- f. indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van gegevens moeten worden gewist;
- g. indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32, lid 1.

Volgens artikel 2.1 jº 2.2 Regeling AVG Defensie ligt de verantwoordelijkheid voor het bijhouden van het verwerkingenregister binnen Defensie bij de AVG-coördinator.

Data Protection Impact Assessment (DPIA)

Artikel 35 lid 1 AVG bepaalt dat de verwerkingsverantwoordelijke vóór een verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt of een verwerking die, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, een beoordeling uitvoert van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Zo'n beoordeling wordt ook wel een gegevensbeschermingseffectbeoordeling of Data Protection Impact Assessment (hierna: DPIA) genoemd. Eén DPIA kan een reeks vergelijkbare verwerkingen beschrijven die vergelijkbare hoge risico's inhouden.

88

Artikel 3 lid 1 Regeling AVG Defensie bepaalt dat de proceseigenaar van een IT-dienst bij de ontwikkeling van een IT-dienst waarmee verwerking van persoonsgegevens is gemoeid die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen; of de betrokken beleidsdirectie bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien, verantwoordelijk zijn voor het initiëren van een DPIA.

Verwerkersovereenkomst

Bij bepaalde activiteiten ontkomt Defensie er niet aan om met externe partijen samen te werken. In die gevallen is het van belang dat Defensie, voorafgaand aan het samenwerken met een externe partij, eerst onderzoekt of de potentiële verwerker voldoende garanties biedt, met name op het gebied van deskundigheid, betrouwbaarheid en middelen, om ervoor te zorgen dat de

technische en organisatorische maatregelen beantwoorden aan de voorschriften van de AVG, mede wat de beveiliging van de verwerking betreft.⁴⁶

Indien een externe partij aan die waarborgen voldoet en Defensie besluit om met die partij in zee te gaan, moet er een verwerkersovereenkomst met die partij worden gesloten. In die overeenkomst worden afspraken gemaakt over het onderwerp en de duur van de verwerking, de aard en de doeleinden van de verwerking, het soort persoonsgegevens en de categorieën van betrokkenen. De verwerkingsverantwoordelijke moet daarbij rekening houden met de specifieke taken en verantwoordelijkheden van de verwerker in het kader van de te verrichten verwerking en het risico in verband met de rechten en vrijheden van de betrokkene.⁴⁷

Ter illustratie: burgers stellen dagelijks vele vragen aan Defensie via sociale media, waaronder YouTube, Facebook, Instagram en Twitter. Om deze vragen centraal te kunnen beantwoorden en niet te hoeven inloggen op vier verschillende accounts, maken medewerkers van de Directie Communicatie gebruik van de softwareapplicatie Coosto. Wanneer vragen via Coosto binnenkomen, worden onder meer de (gebruikers)naam, profielfoto en eventuele andere persoonsgegevens die de burger deelt in zijn vraagstelling verwerkt. Vanwege de verwerking van persoonsgegevens in Coosto, heeft Defensie een verwerkersovereenkomst met deze partij gesloten.

89

5.8 De grondslagen van artikel 6 AVG

Artikel 5 lid 1 sub a AVG bepaalt dat een verwerking van persoonsgegevens rechtmatig moet zijn. Dit houdt in dat er een wettelijke grondslag is vereist voor het verwerken van persoonsgegevens. Deze eis vloeit voort uit het legaliteitsbeginsel, de Grondwet en mensenrechtenverdragen.

De grondslagen voor de verwerking van persoonsgegevens vloeien voort uit artikel 6 lid 1 AVG. De zes grondslagen op basis waarvan gegevensverwerking als rechtmatig kan worden aangemerkt zijn:⁴⁸

- a) *“de betrokkene heeft toestemming gegeven voor de verwerking van zijn persoonsgegevens voor een of meer specifieke doeleinden;*

⁴⁶ Zie artikel 28 lid 1 AVG.

⁴⁷ Zie overweging 81 AVG.

⁴⁸ Voor het verwerken van gewone en gevoelige persoonsgegevens is het voldoende om een grondslag te hebben op basis van artikel 6 lid 1 AVG. Voor het verwerken van bijzondere persoonsgegevens is naast een grondslag op basis van artikel 6 lid 1 AVG ook een doorbrekingsgrond noodzakelijk op grond van artikel 9 lid 2 AVG.

- b) *de verwerking is noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;*
- c) *de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;*
- d) *de verwerking is noodzakelijk om de vitale belangen van de betrokkene of van een andere natuurlijke persoon te beschermen;*
- e) *de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen;*
- f) *de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is."*

In het licht van de activiteiten die Defensie uitvoert zijn niet alle grondslagen relevant. Voor de volledigheid worden ze hieronder wel kort benoemd.

5.8.1 Toestemming betrokkene (sub a)

90

De betrokkene kan toestemming geven voor de verwerking van zijn persoonsgegevens. De toestemming moet vrij zijn gegeven, specifiek, geïnformeerd en ondubbelzinnig zijn (artikel 7 AVG en overweging 32 AVG). Ook moet worden vastgelegd dat toestemming is gegeven. Achteraf moet aangetoond kunnen worden dat er geldige toestemming is verkregen van de betrokkene waarvan persoonsgegevens worden verwerkt. Niet voor elke verwerking is toestemming van betrokkene vereist; er kan ook gebruik gemaakt worden van een van de andere grondslagen die hieronder zijn beschreven.

In artikel 7 van de AVG staan de voorwaarden voor toestemming uitgewerkt. Artikel 7 lid 4 AVG bepaalt dat bij de beoordeling van de vraag of de toestemming vrijelijk kan worden gegeven, onder meer ten sterkste rekening wordt gehouden met de vraag of voor de uitvoering van de overeenkomst, met inbegrip van een dienstenovereenkomst, toestemming vereist is voor een verwerking van persoonsgegevens die niet noodzakelijk is voor de uitvoering van de overeenkomst.

De European Data Protection Board (hierna: EDPB) heeft in overweging 21 van haar Richtsnoeren 05/2020 inzake toestemming overeenkomstig Verordening 2016/679 (vastgesteld op 4 mei 2020) bepaald dat er bij een arbeidsverhouding sprake is van een wanverhouding. Gezien de afhankelijkheid die voortvloeit uit

de relatie tussen werkgever en werknemer, is het onwaarschijnlijk dat de betrokkene zijn werkgever toestemming voor gegevensverwerking zou kunnen weigeren, zonder te hoeven vrezen voor nadelige gevolgen of zich bloot te stellen aan de reële dreiging van nadelige gevolgen. De EDPB is daarom van mening dat het voor werkgevers problematisch is om persoonsgegevens van huidige of toekomstige werknemers te verwerken op basis van toestemming, omdat het onwaarschijnlijk is dat deze vrijelijk wordt verleend. In de meeste gevallen van dergelijke gegevensverwerking op het werk kan en mag de rechtsgrond geen toestemming van de werknemers zijn.

Hoewel medewerkers van Defensie officieel niet worden aangeduid als werknemers, maar als ambtenaren, kan het richtsnoer van de EDPB, vanwege de wel aanwezige gezagsverhouding tussen de overheidsinstantie (Defensie) en de ambtenaar, naar analogie worden toegepast. Dezelfde afhankelijkheidsrelatie (of wanverhouding) is ook aanwezig in de verhouding overheid en burger.⁴⁹ In zijn algemeenheid is het uitgangspunt dat bij een afhankelijke relatie of gezagsverhouding toestemming in beginsel geen geldige grondslag kan zijn.

5.8.2 Uitvoering overeenkomst (sub b)

Het verwerken van persoonsgegevens is gerechtvaardigd, wanneer dit noodzakelijk is voor het uitvoeren van een overeenkomst. Het moet dan wel om een overeenkomst gaan waarbij de betrokkene zelf ook partij is, zoals een overeenkomst fietsplan of een studieovereenkomst tussen Defensie en haar medewerker.

91

5.8.3 Wettelijke verplichting (sub c)

Een verwerking van persoonsgegevens mag worden verricht wanneer de verwerking noodzakelijk is voor de uitvoering van een wettelijke plicht. Deze wettelijke plicht moet blijken uit Unierecht of lidstatelijk recht. In de wet hoeft niet expliciet vermeld te staan dat het noodzakelijk is om persoonsgegevens te verwerken om de wettelijke plicht na te komen. De verplichting kan ruimer geformuleerd zijn. Desondanks moet de verwerking van persoonsgegevens noodzakelijk zijn om aan de wettelijke verplichting te voldoen en moet een individu op basis van de bepaling kunnen voorspellen dat zijn persoonsgegevens worden verwerkt, zodat de organisatie aan de wettelijke verplichting kan voldoen.

Ter illustratie: artikel 4:34 Wet financieel toezicht (hierna: Wft) luidt: “Voor de totstandkoming van een overeenkomst inzake krediet, of een belangrijke

⁴⁹ Zie overweging 42 en 43 AVG.

verhoging van de kredietlimiet, dan wel de som van de bedragen die op grond van een bestaande overeenkomst inzake krediet aan de consument ter beschikking zijn gesteld, wint een aanbieder van krediet in het belang van de consument informatie in over diens financiële positie en beoordeelt hij, ter voorkoming van overkreditering van de consument, of het aangaan van de overeenkomst onderscheidenlijk de belangrijke verhoging verantwoord is."

Deze bepaling uit de Wft verplicht geldverstrekkers om onderzoek te doen naar de financiële draagkracht van de consument. Hoewel de bepaling niet expliciet vermeldt dat er persoonsgegevens verwerkt moeten worden, kan niet aan de verplichting worden voldaan zonder persoonsgegevens te verwerken (noodzakelijkheidsvereiste). De bepaling wordt daarom aangeduid als een wettelijke verplichting.⁵⁰

5.8.4 Vitaal belang (sub d)

Overweging 46 van de AVG bepaalt dat de verwerking van persoonsgegevens ook als rechtmatig wordt beschouwd, indien zij noodzakelijk is voor de bescherming van een belang dat voor het leven van de betrokkene of dat van een andere natuurlijke persoon essentieel is. Verwerking van persoonsgegevens op grond van het vitale belang voor een andere natuurlijke persoon is in beginsel alleen toegestaan indien de verwerking kennelijk niet op een andere rechtsgrond gebaseerd kan worden.

Overweging 112 van de AVG voegt daar aan toe dat onder het vitale belang diens fysieke integriteit of leven wordt verstaan, indien de betrokkene niet in staat is zijn toestemming te geven.

Ter illustratie: deze grondslag kan aan bod komen op het moment dat een medewerker van Defensie bewusteloos raakt en de verwerking van zijn persoonsgegevens noodzakelijk is om het leven van de betreffende medewerker te redden.

5.8.5 Algemeen belang (sub e)

Op grond van artikel 6 lid 1 sub e AVG mogen persoonsgegevens worden verwerkt, wanneer die verwerking noodzakelijk is voor het uitoefenen van een taak van algemeen belang of openbaar gezag. Het moet hierbij gaan om

⁵⁰ Opmerking verdient dat de Hoge Raad prejudiciële vragen heeft gesteld. Uit de prejudiciële beslissing die daarop volgde is gebleken dat de grondslag voor het verwerken van persoonsgegevens in het kader van kredietonderzoek plaatsvindt op grond van artikel 6 lid 1 sub c AVG, maar dat het registreren van persoonsgegevens in het Centraal Krediet Informatie Systeem (hierna: CKI) niet voorzienbaar is op basis van de omschrijving van artikel 4:34 Wft. Voor de registratie van persoonsgegevens in CKI is aansluiting gezocht bij het gerechtvaardigde belang op grond van artikel 6 lid 1 sub f AVG (ECLI:NL:HR:2021:1814).

taken die wettelijk zijn vastgelegd en blijken uit Unierecht of lidstatelijk recht. De AVG schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving is vereist. Er kan worden volstaan met wetgeving die als basis fungeert voor een verwerking die noodzakelijk is voor de vervulling van een taak van algemeen belang of voor een taak in het kader van de uitoefening van het openbaar gezag. In tegenstelling tot de verwerking van persoonsgegevens op grond van artikel 6 lid 1 sub c AVG, moet het bij sub e gaan om een wettelijk vastgelegde taak, in plaats van een verplichting. Uit de taakomschrijving moet ook voortvloeien wie deze taak uitvoert of aan wie het openbaar gezag is opgedragen. Bovendien moet uit de wettelijke taak ook voldoende blijken dat er persoonsgegevens worden verwerkt. Aan de vastlegging van een dergelijke bevoegdheid zijn voorwaarden verbonden. Het verwerken van persoonsgegevens moet noodzakelijk zijn om de taak van algemeen belang of openbaar gezag uit te oefenen. Daarnaast moet de wet duidelijk en nauwkeurig zijn en het moet voor een individu voorspelbaar zijn dat zijn persoonsgegevens worden verwerkt.⁵¹ Dit oordeelde de Hoge Raad tevens in haar uitspraken over het gebruiken van Automatic Numberplate Recognition gegevens (hierna: ANPR) door de Belastingdienst.⁵² Uit artikel 55 Algemene Wet inzake Rijksbelastingen vloeit wel een taak voort, maar geen voldoende precieze grondslag en daarmee bevoegdheid voor het verzamelen, vastleggen, bewaren en gebruiken van de ANPR-gegevens door de Belastingdienst.

Ter illustratie: artikel 3.1 Jeugdwet luidt: "De raad voor de kinderbescherming onderzoekt de noodzaak tot het treffen van een kinderbeschermingsmaatregel, indien het college, een daartoe door het college aangewezen jeugdhulpaanbieder, een gecertificeerde instelling of Veilig Thuis hiertoe een verzoek heeft gedaan."

Uit deze bepaling vloeit een taak voort voor de Raad voor de Kinderbescherming. Voor het uitvoeren van de taak – het onderzoeken van de noodzaak tot het treffen van een kinderbeschermingsmaatregel – is het noodzakelijk om persoonsgegevens te verwerken van het kind. De verwerking van persoonsgegevens is dus voor een betrokkene voldoende voorzienbaar uit de wet.

5.8.6 Algemene opmerkingen over sub c en sub e

Artikel 6 lid 1 sub c en artikel 6 lid 1 sub e AVG bepalen dat de wettelijke plicht, respectievelijk de taak van algemeen belang of openbaar gezag, moet blijken

⁵¹ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 lid 1 sub d AVG.

⁵² Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:286.

uit het Unierecht of het lidstatelijk recht.⁵³ Het is van belang dat het verwerken van persoonsgegevens noodzakelijk is om te voldoen aan de wettelijke plicht of noodzakelijk is om de taak van algemeen belang of openbaar gezag uit te oefenen.

Opmerking verdient dat een taakomschrijving veelal betrekking heeft op één specifieke organisatie of organisatieonderdeel, terwijl een wettelijke verplichting kan gelden voor meerdere organisaties of organisatieonderdelen. Bijvoorbeeld de wettelijke verplichting om onderzoek te doen naar de financiële draagkracht van de consument, voorafgaand aan de kredietverstrekking, geldt voor iedere kredietverstrekker en niet alleen voor banken. Een ander voorbeeld is de taak om de noodzaak tot het treffen van een kinderbeschermingsmaatregel te onderzoeken; deze taak geldt alleen voor de Raad voor de Kinderbescherming. Dat er een taak is toebedeeld aan een organisatie betekent dus niet dat deze organisatie daarmee ook de bevoegdheid heeft om voor die taak persoonsgegevens te verwerken. Bij de grondslag van de wettelijke plicht (artikel 6 lid 1 sub c AVG) en de grondslag van het algemeen belang (artikel 6 lid 1 sub e AVG) is hierbij nog wel specifieke (aanvullende) wetgeving vereist. Uit de wettelijke taak moet dus voldoende duidelijk zijn dat daarbij persoonsgegevens worden verwerkt.⁵⁴ Aan de vastlegging van een dergelijke bevoegdheid of verplichting zijn voorwaarden verbonden. Het verwerken van persoonsgegevens moet noodzakelijk zijn om de taak van algemeen belang of openbaar gezag uit te oefenen. Daarnaast moet de wet moet duidelijk en nauwkeurig zijn en het moet voor een individu voorspelbaar zijn dat zijn persoonsgegevens worden verwerkt.⁵⁵

5.8.7 Gerechtvaardigd belang (sub f)

Er zijn gevallen waar de verwerkingsverantwoordelijke geen beroep kan doen op de grondslagen a t/m e uit artikel 6 lid 1 AVG. Als de verwerkingsverantwoordelijke alsnog persoonsgegevens wil verwerken kan mogelijk aansluiting worden gezocht bij grondslag f van artikel 6 lid 1 AVG; het gerechtvaardigd belang. Artikel 6 lid sub f AVG luidt als volgt:

“De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan: de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen

⁵³ Zie overweging 41 en 45 van de AVG.

⁵⁴ Zie Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:286. In deze uitspraak oordeelde dat de Hoge Raad dat de Belastingdienst op grond van artikel 55 Algemene wet inzake rijksbelastingen geen voldoende precieze grondslag heeft voor het verzamelen, vastleggen, bewaren en gebruiken van de ANPR-gegevens.

⁵⁵ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 lid 1 sub d AVG.

of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is."

Uit dit artikel komt naar voren dat er een belangenafweging plaats moet vinden tussen het belang van de verwerkingsverantwoordelijke en de betrokkene. Er is namelijk een botsing van rechtsbelangen; het grondrecht van de betrokkene tegen het (grond)recht van de verwerkingsverantwoordelijke of derde. Op basis van artikel 6 lid 1 sub f AVG zijn er drie cumulatieve vereisten waaraan moet worden voldaan voor een gerechtvaardigd belang:

1. Gerechtvaardigd

Het gerechtvaardigde belang moet in (algemene) wetgeving of elders in het recht zijn benoemd als een rechtsbelang. De verwerkingsverantwoordelijke of derde moet zich dus op een (geschreven of ongeschreven) rechtsregel of rechtsbeginsel kunnen beroepen. Tegelijkertijd zegt die rechtsregel of dat rechtsbeginsel niets, of niet genoeg, over de verwerking van persoonsgegevens. Hierdoor is die rechtsregel of dat rechtsbeginsel voor de betrokkene niet (voldoende) duidelijk en nauwkeurig over de verwerking van persoonsgegevens en/of de toepassing ervan is (onvoldoende) voorspelbaar. Dat heeft als gevolg dat verwerking op basis van de c of e-grondslag niet mogelijk is. Wat niet als gerechtvaardigd belang kwalificeert, is een algemeen belang van 'de samenleving' of iets dergelijks. Het belang moet namelijk wel concreet zijn.

95

2. Noodzakelijk

Op het moment dat het belang gerechtvaardigd is, moet de verwerking van persoonsgegevens ook noodzakelijk zijn om het belang te behartigen. De verwerkingsverantwoordelijke moet toetsen aan de eisen van proportionaliteit en subsidiariteit.

3. Belangenafweging

De verwerkingsverantwoordelijke moet een belangenafweging uitvoeren tussen de belangen van de betrokkene enerzijds en de belangen van de verwerkingsverantwoordelijke anderzijds. Deze belangenafweging moet worden vastgelegd om te voldoen aan de verantwoordingsplicht. Op die manier is op een later tijdstip ook reproduceerbaar welke belangen zijn meegewogen en kan bij een verzoek van een betrokkene ook getoetst worden of de belangen van de betrokkene in een specifiek geval zwaarder wegen dan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke.

De grondslag gerechtvaardigd belang kan dus alleen worden toegepast wanneer deze gerechtvaardigd belang toets is uitgevoerd en de belangenafweging in het voordeel uitvalt van de verwerkingsverantwoordelijke.

5.8.8 Gerechtvaardigd belang voor overheidsinstanties

Overheidsinstanties, zoals het Ministerie van Defensie, mogen zich bij het uitoefenen van hun (wettelijke) taken niet beroepen op de grondslag gerechtvaardigd belang. Dit blijkt uit de laatste volzin van artikel 6 lid 1 sub f AVG.⁵⁶ Een beroep op het gerechtvaardigd belang door een overheidsinstantie is alleen mogelijk wanneer er sprake is van een verwerking van persoonsgegevens bij een typisch bedrijfsmatige handeling. Een voorbeeld van een typisch bedrijfsmatige handeling voor een overheidsinstantie is de toegangsbeveiliging bij overheidsgebouwen.⁵⁷ Naast het voorbeeld over toegangsbeveiliging wordt er in de literatuur en de rechtspraak helaas geen nadere uitleg gegeven over typisch bedrijfsmatige handelingen van overheidsinstanties. Ook in de 'normuitleg gerechtvaardigd belang (november 2019)' van de Autoriteit Persoonsgegevens wordt het gerechtvaardigd belang vanuit overheidsperspectief niet nader belicht.⁵⁸

96

De Groep Gegevensbescherming Artikel 29 heeft op 9 april 2014 wel een advies uitgebracht over het begrip 'gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke' in artikel 7 van Richtlijn 95/46/EG. Hoewel Richtlijn 95/46/EG met de inwerkingtreding van de AVG is ingetrokken, is in het advies ook vooruitgeblikt op de AVG. Over artikel 6 lid 1 sub f AVG zegt de Groep Gegevensbescherming Artikel 29 het volgende:

"De desbetreffende laatste zin van artikel 6, lid 1, onder f), van de voorgestelde verordening kan ook zo worden geïnterpreteerd dat overheidsinstanties niet volledig worden uitgesloten van het gebruik van het gerechtvaardigd belang als rechtsgrond. In dit geval moet de zinsnede "verwerking door overheidsinstanties in het kader van de uitoefening van hun taken" in het voorgestelde artikel 6, lid 1, onder f), strikt worden geïnterpreteerd. Deze strikte interpretatie zou inhouden dat de verwerking voor het behoorlijke beheer en de werking van deze overheidsinstanties buiten het toepassingsgebied zou vallen van "verwerking door overheidsinstanties in het kader van de uitoefening van hun taken". Als gevolg hiervan zou de verwerking voor het behoorlijke beheer

⁵⁶ De laatste volzin van artikel 6 lid 1 sub f AVG bepaalt: "De eerste alinea, punt f), geldt niet voor de verwerking door overheidsinstanties in het kader van de uitoefening van hun taken."

⁵⁷ De Vries, in: *T&C Privacy- en gegevensbescherming*, aantekening bij artikel 6 AVG.

⁵⁸ Zie

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/normuitleg_gerechtvaardigd_belang.pdf

en de werking van deze overheidsinstanties nog steeds mogelijk zijn overeenkomstig de grond van gerechtvaardigd belang."⁵⁹

In het licht van dit advies zijn wij van mening dat activiteiten met betrekking tot HR, financiën, interne audit, marketing, communicatie, inkoop en beveiliging typisch bedrijfsmatige handelingen kunnen zijn voor een overheidsinstantie. Uiteraard is het afhankelijk van alle omstandigheden van de precieze handeling of de overheidsinstantie ook daadwerkelijk een succesvol beroep kan doen op het gerechtvaardigd belang. Binnen de overheid ontbreken hier momenteel duidelijke kaders en richtlijnen voor. Om te voorkomen dat overheidsinstanties, waaronder Defensie, als het ware misbruik kunnen maken van de grondslag gerechtvaardigd belang is het essentieel dat de overheid duidelijke en strikte voorschriften en richtlijnen maakt. Daarbij is ook van belang om de doelbinding van deze verwerkingen nauwgezet te omschrijven en verdere verwerking te limiteren.

Een overheidsinstantie als Defensie kan bijvoorbeeld wel een beroep doen op het gerechtvaardigd belang voor het verwerken van persoonsgegevens bij het uitvoeren van toegangscontroles op defensie terreinen. Bij de toegangscontrole vraagt de beveiliging van Defensie om het identiteitsbewijs van de bezoeker en voert hij persoonsgegevens in het systeem in.⁶⁰ Het uitvoeren van een toegangscontrole kan worden aangemerkt als een typisch bedrijfsmatige handeling, waarvoor een beroep kan worden gedaan op de rechtsgrondslag gerechtvaardigd belang.

97

5.9 Toepasselijke wet- en regelgeving voor Defensie

In paragraaf 5.8 is opgemerkt dat de wettelijke plicht, respectievelijk de taak van algemeen belang of openbaar gezag, moet blijken uit het Unierecht of het lidstatelijk recht voor een succesvol beroep op artikel 6 lid 1 sub c en artikel 6 lid 1 sub e AVG. Artikel 10 lid 1 Gw bepaalt dat de bevoegdheid voor het verwerken van persoonsgegevens alleen kan worden afgeleid uit een wet in

⁵⁹ Groep Gegevensbescherming Artikel 29, in: Advies 06/2014 over het begrip "gerechtvaardigd belang van de voor de gegevensverwerking verantwoordelijke" in artikel 7 van Richtlijn 95/46/EG, vastgesteld op 9 april 2014. Paragraaf III.2.5. Taak van algemeen belang, p. 28.

⁶⁰ Bij het uitvoeren van de toegangscontrole moet worden opgemerkt dat de beveiliging van Defensie niet zonder meer het Burgerservicenummer mag verwerken. Een overheidsinstantie mag alleen dan het Burgerservicenummer verwerken, wanneer dat voor het specifieke geval noodzakelijk is en dit wettelijk is vastgelegd. Bij toegangscontroles worden persoonsgegevens verwerkt voor het identificeren van de bezoeker. Deze identificatie kan ook plaatsvinden zonder verwerking van het Burgerservicenummer.

formele zin.⁶¹ Dat er sprake moet zijn van een formeel wettelijke basis blijkt ook uit een uitspraak van de Hoge Raad, waarin is opgenomen dat "(...) de woorden "behoudens bij of krachtens de wet te stellen beperkingen" in artikel 10 van de Grondwet brengen bovendien mee dat beperkingen op het recht op eerbiediging van de persoonlijke levenssfeer slechts kunnen worden gerechtvaardigd door of krachtens een wet in formele zin(...)".⁶²

De Raad van State volgt deze lijn ook in haar voorstel inzake de Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid.⁶³ Een taak die volgt uit een wet in materiële zin, zoals het Algemeen organisatiebesluit Defensie 2021 of een daaronder liggend subtaakbesluit, kan voor Defensie op zichzelf dus nog geen wettelijke basis vormen voor een rechtmatige verwerking van persoonsgegevens. De bevoegdheid voor het verwerken van persoonsgegevens kan alleen worden afgeleid uit een wet in formele zin.

De taken en verplichtingen voor Defensie en rechten en plichten voor ambtenaren van Defensie en dienstplichtigen vloeien voort uit verschillende wetten. In deze paragraaf volgt een opsomming van een aantal voorbeelden van wetten die voor Defensie relevant kunnen zijn.⁶⁴

98

5.9.1 De Grondwet

Artikel 44 lid 1 Gw bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministeries staan onder leiding van een minister. Uit deze bepaling vloeit voort dat het Ministerie van Defensie ook is ingesteld bij koninklijk besluit. Uit dit artikel volgen geen taken en bevoegdheden voor Defensie.

Artikel 97 lid 1 Gw bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

⁶¹ Zie in dit kader de MvT bij wetsvoorstel Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid, Kamerstukken 35958-3, p. 24.

⁶² Hoge Raad 24 februari 2017, ECLI:NL:HR:2017:288 rechtsoverweging 2.3.2.

⁶³ Raad van State No. W16.21.0218/II.

⁶⁴ Opmerking vooraf: niet iedere wet in deze opsomming kwalificeert als een wet in formele zin. Dit brengt met zich mee dat er niet zonder meer sprake is van een publieke taak in de zin van artikel 6 lid 1 sub e AVG. Daarnaast biedt niet iedere taakomschrijving een grondslag voor het verwerken van persoonsgegevens. Of daarvan sprake is komt bij de uitgebreide beoordeling van de activiteiten (bijlage) aan bod.

Hoewel uit de Memorie van Toelichting op artikel 97 Gw wel blijkt wat de doelstellingen zijn van de krijgsmacht, valt de verwerking van persoonsgegevens bij de uitoefening van de beleidsmatig vastgestelde taken ten behoeve van deze doelstellingen buiten de materiële werkingssfeer van de AVG, voor zover de Minister van Defensie daartoe beslist in het kader van inzet of het ter beschikking stellen van de krijgsmacht (zie paragraaf 5.5). Voor zover de verwerking van persoonsgegevens bij de uitvoering van de taken uit artikel 97 Gw wel onder de AVG valt, merken wij op dat de taakomschrijving van artikel 97 Gw onvoldoende concreet, duidelijk en specifiek is om daaruit te kunnen afleiden dat er persoonsgegevens kunnen worden verwerkt bij de uitvoering van de taken. Uit artikel 97 Gw kan dan ook geen specifieke taak noch een specifieke bevoegdheid tot het in dat verband verwerken van persoonsgegevens worden afgeleid.

Uit de grondwet vloeien ook andere verplichtingen voort, zoals de plicht tot het verstrekken van inlichtingen (artikel 68 Gw).

5.9.2 De Politiewet 2012

Hoofdstuk 2 van de Politiewet 2012 (hierna: Politiewet) omschrijft de uitvoering van de politietaak. In paragraaf 2.1 worden de taken van de politie en de politietaken van de KMar opgesomd en in paragraaf 2.2 worden de bevoegdheden weergegeven. Voor de KMar, als krijgsmachtonderdeel van Defensie, is met name artikel 4 Politiewet relevant. Dat artikel geeft namelijk de politietaken van de KMar weer. Met betrekking tot de militaire bijstandstaken van de KMar en andere krijgsmachtonderdelen zijn ook artikel 57 tot en met 59 Politiewet en artikel 51 Wet veiligheidsregio's van toepassing. Voor zover deze taken buiten de reikwijdte van de Richtlijn gegevensbescherming politie en justitie⁶⁵ vallen, kan de taakomschrijving als grondslag cq bevoegdheid dienen voor het verwerken van persoonsgegevens op grond van artikel 6 lid 1 sub e AVG. Nu er sprake is van een wet in formele zin. Voor zover het gaat om taken buiten de reikwijdte van de AVG vormen artikel 2 Wpg jo. artikelen 8 tot en met 13 Wpg een grondslag voor het verwerken van persoonsgegevens door de KMar. Voorwaarde daarbij is wel dat de taakomschrijving voldoende concreet is én dat het voor een betrokkene voorzienbaar is dat zijn persoonsgegevens bij het uitvoeren van de taak kunnen worden verwerkt. Voor zover relevant wordt dit bij de uitgebreide beoordeling van de activiteiten verder uitgewerkt.

⁶⁵ Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende gegevensbescherming politie en justitie (PbEU 2016, L 119/89).

5.9.3 De Wet veiligheidsregio's

Artikel 19 lid 1 van de Wet veiligheidsregio's bepaalt dat het bestuur van de veiligheidsregio's, de korpschef en de hoofdofficier van justitie een convenant sluiten met het oog op de samenwerking bij branden, rampen en crises. Een convenant dat betrekking heeft op de door de KMar uitgeoefende politietaak wordt gesloten met Onze Minister van Defensie. Artikel 20 lid 1 van de Wet veiligheidsregio's voegt hieraan toe dat bij ministeriële regeling regels kunnen worden gesteld over de samenwerking tussen veiligheidsregio's en tussen veiligheidsregio's en de politie en de KMar indien het de uitoefening van een politietaak betreft.

Daarnaast bepaalt artikel 51 van de Wet veiligheidsregio's dat Onze Minister zich met een verzoek om militaire bijstand kan richten tot Onze Minister van Defensie.

Voor zover er bij de activiteiten die binnen de reikwijdte van dit onderzoek vallen persoonsgegevens worden verwerkt in het kader van de in de Wet veiligheidsregio's opgenomen taken, komt dit bij de uitgebreide beoordeling van de activiteiten verder aan bod.

5.9.4 Rijkswet geweldgebruik bewakers militaire objecten

100

De Rijkswet geweldgebruik bewakers militaire objecten (hierna: Rijkswet) schept kaders voor militairen en burgermedewerkers belast met de bewakings- en beveiligingstaken waarbinnen zij gebruik mogen maken van geweld ter bescherming van militaire objecten. De wettelijke verankering hiervan vloeit voort uit artikel 11 Gw. Dit artikel verzekert de onaantastbaarheid van het menselijk lichaam. Een beperking van dit grondrecht moet bij of krachtens wet geschieden. Om die reden is er een wet in formele zin gecreëerd, zijnde de Rijkswet.

Voor zover er bij de activiteiten die binnen de reikwijdte van dit onderzoek vallen persoonsgegevens worden verwerkt in het kader van de Rijkswet, komt dit bij de uitgebreide beoordeling van de activiteiten verder aan bod.

5.9.5 De Wet ambtenaren Defensie

De Wet ambtenaren Defensie regelt de rechtspositie en geeft rechten en plichten aan ambtenaren van Defensie, waaronder het recht om een klacht in te dienen over krenkende of onbillijke behandeling door een meerdere (artikel 9 lid 1), de plicht tot goed werkgever- en werknemerschap (artikel 12bis), de plicht tot het afleggen van de eed of de belofte (artikel 12quater lid 1), de

beperking op de vrijheid van meningsuiting (artikel 12a lid 1) en de beperking op het recht om te staken (artikel 12i lid 1).

Voor zover er bij de activiteiten die binnen de reikwijdte van dit onderzoek vallen persoonsgegevens worden verwerkt in het kader van de uitoefening van de rechten van de ambtenaar van Defensie, komt dit bij de uitgebreide beoordeling van de activiteiten verder aan bod.

5.9.6 De Kaderwet dienstplicht

De Kaderwet dienstplicht geeft regels over de dienstplicht, waaronder de inschrijving, de keuring, de rechtstoestand van de dienstplichtige en de uitoefening van de grondrechten door de dienstplichtige. Hiermee geeft de Kaderwet dienstplicht een nadere invulling aan de rechten en plichten van dienstplichtigen.

Voor zover er bij de activiteiten die binnen de reikwijdte van dit onderzoek vallen persoonsgegevens worden verwerkt in het kader van de uitoefening van de rechten van de dienstplichtige, komt dit bij de uitgebreide beoordeling van de activiteiten verder aan bod.

5.9.7 Algemeen organisatiebesluit Defensie 2021

Het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) is een zelfstandig ministeriële regeling die niet op een expliciete delegatiegrondslag berust. De tweede volzin van artikel 44 lid 1 Gw bepaalt dat ministeries onder leiding staan van een minister. Uit deze volzin blijkt de impliciete grondslag voor de minister om de inrichting van het ministerie te bepalen. In dat licht heeft de Minister van Defensie het AOD vastgesteld, waarin de verschillende taken en functies van de DO'en zijn neergelegd. Hoewel het AOD als een taakomschrijving is geformuleerd, kan hier geen bevoegdheid tot het verwerken van persoonsgegevens in de zin van artikel 6 lid 1 sub e AVG worden ontleend, omdat het AOD niet kwalificeert als een wet in formele zin. Het AOD is aan te merken als een intern inrichtingsbesluit.

5.9.8 Subtaakbesluiten

Artikel 26 AOD bepaalt dat de verantwoordelijken uit artikel 1 AOD op basis van dit besluit subtaakbesluiten kunnen vaststellen ten aanzien van de eenheden waaraan zij leidinggeven. Deze subtaakbesluiten worden vastgesteld na goedkeuring door de Secretaris-Generaal of, indien de Secretaris-Generaal het subtaakbesluit vaststelt, na goedkeuring door de Minister van Defensie.

Uit artikel 26 AOD blijkt een discretionaire bevoegdheid. Dit houdt in dat verantwoordelijken de keuzevrijheid hebben om een subtaakbesluit vast te

stellen. Zij zijn hier dus niet toe verplicht. Een subtaakbesluit wordt aangemerkt als een beleidsregel of een ministeriële regeling.

Een subtaakbesluit is geen wet in formele zin, waardoor er geen bevoegdheid tot het verwerken van persoonsgegevens aan kan worden ontleend op basis van artikel 6 lid 1 sub e AVG. Net als het AOD is een subtaakbesluit aan te merken als een intern inrichtingsbesluit.

Bijlage 1 Omschrijving activiteiten

In de onderstaande tabel een overzicht van alle activiteiten en of deze ten tijde van het onderzoek plaatsvond.

Activiteit voldoet volledig aan de AVG en vond plaats tijdens het onderzoek, eventuele aanbevelingen blokkeren de doorgang niet	Activiteit met knelpunt(en), maar de betreffende activiteit vindt niet, niet meer of nog niet plaats	Activiteiten met knelpunten die tijdens het onderzoek plaatsvonden. Dit moet voor een aantal activiteiten geverifieerd worden.
3	6	1
4	7	2
11	8	5
12	9A	10B
13	9B	14A
15	10A	14B
16		17
18		19
20		
21		
22		
5A		

Activiteit 1

Omschrijving activiteit 1

Het is voor de Minister van Defensie van belang om op de hoogte te zijn van wat er – op het gebied van Defensie – speelt in de maatschappij. In deze informatiebehoefte kan onder meer worden voorzien door middel van werkbezoeken en Kamerdebatten. Ook de Directie Communicatie (hierna: DCo) draagt bij aan het vervullen van deze informatiebehoefte, door mediaberichten te monitoren, te signaleren en te duiden.

DCo houdt zich bezig met diverse activiteiten. Eén van die activiteiten is het monitoren, signaleren en duiden van mediaberichten voor communicatiedoeleinden. DCo monitort via onder meer LexisNexis mediaberichten die voor communicatiemedewerkers en voor de top van Defensie relevant zijn. De mediaberichten die DCo monitort zijn berichten over Defensie of over onderwerpen die gerelateerd zijn aan Defensie. Indien DCo relevante mediaberichten signaleert, worden deze samengevat of opgenomen in de Nieuwsupdate. De meest relevante mediaberichten worden opgenomen in de dagelijkse Nieuwsbrief (ook wel aangeduid als: Knipselkrant). De Nieuwsupdate en de Nieuwsbrief/Knipselkrant worden dagelijks voor zeven dagen op het intranet gepubliceerd en naar bepaalde verzendgroepen verstuurd, waaronder een verzendgroep bestaande uit de communicatiemedewerkers van Defensie. De ontvangers in deze verzendgroepen zijn allen medewerkers van Defensie en beschikken vanuit die hoedanigheid over een @mindef-account. Indien een medewerker van DCo behoefte heeft aan een overzicht van mediaberichten, kan de betreffende medewerker de Nieuwsroom van DCo verzoeken om een overzicht aan te leveren. Eventuele trends in die mediaberichtgeving kunnen door DCo in dat overzicht worden geduid.

104

Omdat de Nieuwsupdate bestaat uit samenvattingen van relevante oorspronkelijke mediaberichten, kan het zijn dat er sprake is van een verwerking van persoonsgegevens, zoals namen van journalisten of andere tot personen te herleiden gegevens die in de mediaberichten worden genoemd. Het verwerken van deze persoonsgegevens vindt te allen tijde plaats voor de interne en externe communicatiedoelen in het kader van de goede uitvoering van de beleids-, beheers- en bestuurstaken en verantwoordelijkheden van het Ministerie van Defensie.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DCO, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het

Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 68 van de Grondwet (hierna: Gw) geeft de inlichtingenplicht weer.

“De ministers en staatssecretarissen geven de kamers elk afzonderlijk en in verenigde vergadering mondeling of schriftelijk de door een of meer leden verlangde inlichtingen waarvan het verstrekken niet in strijd is met het belang van de staat.”

Het parlement kan zijn controle- en medewetgevingstaken alleen adequaat uitvoeren, als het over de daartoe noodzakelijke informatie beschikt. Daarom zijn bewindslieden gehouden inlichtingen te verstrekken wanneer een Kamerlid of de Kamer daarom verzoekt. Deze regel is opgenomen in artikel 68 Gw en vloeit voort uit de verantwoordingsplicht voor ministers en staatssecretarissen die in het parlementaire stelsel ligt opgesloten.

Algemeen organisatiebesluit Defensie 2021

Artikel 7 van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) bepaalt het volgende.

“De Directeur Communicatie is belast met:

- 1. Het met inachtneming van de aanwijzingen van de Secretaris-Generaal geven van ambtelijke leiding aan de Directie Communicatie;*
- 2. De woordvoering namens de politieke, ambtelijke en militaire leiding, voor zover het de verantwoordelijkheid van de Minister van Defensie betreft;*
- 3. Het gevraagd en ongevraagd adviseren van de politieke, ambtelijke en militaire leiding inzake mediagevoelige aangelegenheden;*
- 4. De externe, interne en arbeidsmarktcommunicatie;*
- 5. Het ontwikkelen, coördineren en handhaven van integraal en uitvoerend communicatiebeleid in afstemming met de Directeur-Generaal Beleid en de Rijksvoorlichtingsdienst.”*

105

Wij zijn van mening dat deze activiteit geschaard kan worden onder de taak uit artikel 7 sub c AOD.

Toepassingsbereik AVG

Materieel toepassingsbereik

Dco monitort en raadpleegt mediaberichten via geautomatiseerde systemen én verwerkt mediaberichten in een nieuw document, zoals de zogeheten Nieuwsupdate. Er is dus sprake van een verwerking van persoonsgegevens in de zin van artikel 2 AVG.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

De AVG is dus wel van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. In deze paragraaf lichten wij de relevante grondslagen toe.

106

Wettelijke plicht

Artikel 6 lid 1 sub c AVG bepaalt dat een verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is om te voldoen aan een wettelijke verplichting.

Uit overweging 45 van de AVG volgt dat de verwerking voor een succesvol beroep op artikel 6 lid 1 sub c AVG of artikel 6 lid 1 sub e AVG een grondslag moet hebben in een Unierechtelijke of lidstaatrechtelijke bepaling. Overweging 41 van de AVG voegt daaraan toe dat de rechtsgrond of wetgevingsmaatregel evenwel duidelijk en nauwkeurig moet zijn, en de toepassing daarvan voorspelbaar moet zijn voor degenen op wie deze van toepassing is.

Daarnaast bepaalt artikel 10 Gw dat een overheidsinstantie zich in beginsel niet mag inmengen in de persoonlijke levenssfeer van een burger, tenzij een wet in formele zin hiervoor een grondslag biedt én die wet regels stelt voor het beschermen van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens.

Bij onze zoektocht naar een eventuele wettelijke plicht zijn wij gestuit op artikel 68 Gw. Dat artikel geeft de inlichtingenplicht weer. Hoewel de Grondwet een

wet in formele zin is, zijn wij van mening dat uit deze bepaling niet kan worden afgeleid dat ministers en staatssecretarissen bij het verstrekken van (schriftelijke) inlichtingen ook persoonsgegevens kunnen verwerken. Hierdoor wordt niet voldaan aan het vereiste van duidelijkheid, nauwkeurigheid en voorspelbaarheid, zoals genoemd in overweging 41 van de AVG.

Daarnaast betreft artikel 68 Gw een passieve verplichting is, die geen continue monitoring vereist, zoals bij de Newsroom het geval is. Gelet daarop komen wij tot de conclusie dat een eventueel beroep op artikel 6 lid 1 sub c AVG bij deze activiteit geen kans van slagen heeft.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat een verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen.

Hetgeen hiervoor, met verwijzing naar overweging 41 en 45 van de AVG en artikel 10 Gw is opgemerkt over artikel 6 lid 1 sub c AVG, is van overeenkomstige toepassing op artikel 6 lid 1 sub e AVG. Dit brengt met zich mee dat de taak van algemeen belang ook moet voortvloeien uit een Unierechtelijke of lidstaatrechtelijke bepaling.

107

In de vorige paragraaf hebben wij opgemerkt dat deze activiteit volgens ons geschaard kan worden onder de taakomschrijving van artikel 7 sub c AOD. Het verwerken van persoonsgegevens in een Nieuwsupdate en/of Nieuwsoverzicht draagt namelijk bij het aan gevraagd en ongevraagd adviseren van de politieke, ambtelijk en militaire leiding inzake mediagevoelige aangelegenheden.

Wij zijn echter van mening dat artikel 6 lid 1 sub e AVG niet als grondslag kan dienen voor de verwerking van persoonsgegevens in een Nieuwsupdate en/of Nieuwsoverzicht, omdat het AOD niet kan worden aangemerkt als een lidstaatrechtelijke bepaling met formele rechtskracht. Daarnaast is uit de taakomschrijving van artikel 7 sub c AOD onvoldoende voorzienbaar dat DCo, bij de uitvoering van haar taak, persoonsgegevens kan verwerken, waardoor niet aan het vereiste van duidelijkheid, nauwkeurigheid en voorspelbaarheid wordt voldaan. Wij zijn dan ook van mening dat een succesvol beroep op artikel 6 lid 1 sub e AVG bij deze activiteit – onder de huidige omstandigheden – geen kans van slagen heeft.

Gerechtvaardigd belang

Artikel 6 lid 1 sub f AVG bepaalt dat de verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De laatste volzin van artikel 6 lid 1 sub f AVG voegt daaraan toe dat overheidsinstanties in het kader van de uitoefening van hun taken geen beroep kunnen doen op artikel 6 lid 1 sub f AVG.

In hoofdstuk 5 van dit rapport hebben wij uiteengezet dat een beroep op het gerechtvaardigd belang door overheidsinstanties alleen mogelijk is voor typisch bedrijfsmatige handelingen van die overheidsinstanties. Wij zijn van mening dat activiteiten met betrekking tot HR, financiën, control, marketing, communicatie, inkoop en beveiliging typische bedrijfsmatige handelingen kunnen zijn voor overheidsinstanties.

Wij zijn van mening dat het verwerken van persoonsgegevens in een Nieuwsupdate en/of Nieuwsbrief, met als doel om de politieke, ambtelijke en militaire leiding gevraagd en ongevraagd te adviseren inzake mediagevoelige aangelegenheden geschaard kan worden onder communicatie. Wij durven echter niet te stellen dat het verwerken van persoonsgegevens in een Nieuwsupdate en/of Nieuwsbrief kwalificeert als een typisch bedrijfsmatige handeling voor een overheidsinstantie als Defensie. Alvorens de in artikel 6 lid 1 sub f AVG vereiste belangenafweging te maken, doet Defensie er volgens ons goed aan om nader onderzoek te verrichten naar de definitie van het begrip 'typisch bedrijfsmatige handeling voor overheidsinstanties'.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Voor een mogelijk succesvol beroep op artikel 6 lid 1 sub e AVG ontbreekt een duidelijke, nauwkeurige en voorspelbare taakomschrijving, welke is vastgelegd in een wet in formele zin.	Het formuleren van een duidelijke, nauwkeurige en voorspelbare taakomschrijving voor het verwerken van persoonsgegevens door DCo en deze taakomschrijving vastleggen in een wet in formele zin.
2.	Voor een mogelijk succesvol beroep op artikel 6 lid 1 sub f AVG ontbreekt een eenduidige definitie van 'typische bedrijfsmatige handelingen voor	Het opstellen van een beleidsstuk waarin wordt vastgelegd wat volgens Defensie wordt aangemerkt als een typisch bedrijfsmatige handeling. Indien dat nader is uitgekristalliseerd

	overheidsinstanties' en de vereiste belangenafweging.	vereist artikel 6 lid 1 sub f nog een belangenafweging voor het verwerken van persoonsgegevens in deze activiteit.
--	---	--

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

Artikel 12 AVG bepaalt dat een betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in een duidelijke, eenvoudige taal moet worden geïnformeerd over de onderwerpen genoemd in artikel 14 AVG.

Respondent heeft aangegeven dat journalisten op de hoogte zijn van de verwerking van hun publicaties in LexisNexis vanwege een overeenkomst die tussen de journalisten of hun uitgeverijen en LexisNexis is gesloten. Daarnaast worden journalisten via de website van Defensie geïnformeerd over de verwerking van hun persoonsgegevens.⁶⁶ Wij merken op dat voor journalisten aan het transparantiebeginsel wordt voldaan.

109

Dit is voorsnog anders voor de personen wiens persoonsgegevens in de mediaberichten worden genoemd. Strikt juridisch gezien moeten deze betrokkenen op grond van artikel 14 AVG ook worden geïnformeerd over de verwerking van hun persoonsgegevens. Het is echter onwenselijk als DCo iedere betrokkene op persoonsniveau moet informeren over de verwerking van haar persoonsgegevens bij de interne verwerking van reeds gepubliceerde mediaberichten.

Artikel 14 lid 5 AVG biedt enkele mogelijkheden om af te wijken van de informatieplicht. Artikel 14 lid 5 sub b AVG bepaalt dat de informatieplicht uit de leden 1 tot en met 4 van artikel 14 AVG niet van toepassing is wanneer en voor zover het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning vergt, voor zover de in artikel 14 lid 1 AVG bedoelde verplichting de

⁶⁶ Zie "Hoe gaat Defensie om met de persoonsgegevens van journalisten?" | Privacyrechten | Defensie.nl

verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen.⁶⁷

Wij merken op dat het (op individuele basis) informeren van iedere betrokkene een dusdanig onevenredige inspanning vergt, dat het opstellen van de Nieuwsupdate en/of Nieuwsbrief onmogelijk wordt. Op het moment dat een betrokkene, zoals een publiek figuur, persoonlijk is geïnformeerd, bestaat de kans dat het betreffende mediabericht al niet meer actueel is. Het bereiken en informeren van de betreffende betrokkene kan namelijk de nodige tijd in beslag nemen. Ondanks deze onevenredige inspanning zijn wij van mening dat betrokkenen wel op algemene wijze geïnformeerd kunnen worden, door middel van de privacyverklaring op de website.

Verder vereist artikel 14 lid 5 sub b AVG dat de verwerkingsverantwoordelijke passende maatregelen neemt om de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van informatie. Hierover merken wij op dat DCo de persoonsgegevens niet openbaar maakt, beperkte verzending en publicatie, en beveiliging volgens het DBB als waarborgen heeft ingebouwd.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
3.	Betrokkenen kunnen op algemene wijze beter worden geïnformeerd over de (sociale) mediamonitoring door DCo.	Het toevoegen van een passage over (sociale) mediamonitoring in de privacyverklaring.

Hoewel wij van mening zijn dat betrokkenen niet op individuele basis geïnformeerd hoeven worden, kunnen zij op algemene wijze wel beter worden geïnformeerd door het toevoegen van een passage in de privacyverklaring. Wij zijn dan ook van mening dat aan het beginsel van behoorlijkheid en transparantie nog niet volledig wordt voldaan.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

⁶⁷ Overweging 62 van de Richtsnoeren inzake transparantie overeenkomstig Verordening (EU) 2016/679 d.d. 11 april 2018 bepaalt dat de onmogelijkheid of onevenredige inspanning rechtstreeks verband moet houden met het feit dat de persoonsgegevens niet van de betrokkene zijn verkregen.

Bij het uitvoeren van de aan DCo opgedragen taken is een van de activiteiten het monitoren, signaleren en duiden van mediaberichten voor communicatiedoeleinden. De taken en communicatiedoeleinden zijn neergelegd in het interne beleidsstuk '*Corporate Visie op Communicatie*'. De communicatiedoeleinden die hieruit voortvloeien zijn:

1. het communiceren met en verantwoording afleggen aan de eigen medewerkers en de samenleving;
2. het bouwen aan vertrouwen van de eigen medewerkers en de Nederlandse burgers;
3. het uitbouwen, behouden en creëren van de in- en extern draagvlak voor (de taken van) de krijgsmacht;
4. het positioneren van Defensie als betrouwbare en aantrekkelijke werkgever;
5. het positioneren van Defensie als aantrekkelijke partner voor relevante organisaties in de samenleving (bedrijfsleven, zorg, onderwijs).

Uit de Data Protection Impact Assessment (hierna: DPIA) Uitvoeren communicatiebeleid, (sociale) mediamonitoring blijkt dat voor (sociale) mediamonitoring de volgende doelen zijn vastgesteld:

1. vroegsignalering ten behoeve van issuemanagement door signalering (ex ante): volgen van discussies over Defensie en/of Defensie gerelateerde onderwerpen in relevante arena's. Zien welke vragen/zorgen er zijn over deze onderwerpen;
2. (realtime) signalering: wat is de actuele berichtgeving over Defensie en/of Defensie gerelateerde onderwerpen in relevante arena's. Dit omdat berichtgeving feitelijk onjuist kan zijn en mogelijk moet worden aangepast. Voorbereid zijn op vragen die naar aanleiding van de berichtgeving aan Defensie kunnen worden gesteld;
3. evalueren (ex post): hoe worden Defensie communicatieboodschappen ontvangen en kan Defensie hier lessen uit trekken voor de toekomst?

111

Onzes inziens kan deze activiteit niet plaatsvinden zonder de verwerking van de in het mediabericht voorkomende persoonsgegevens. Wij zijn dan ook van mening dat aan het beginsel van doelbinding wordt voldaan.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

DCo verwerkt alleen de persoonsgegevens die in de mediaberichten voorkomen. Nader onderzoek naar in de mediaberichten voorkomende

personen wordt niet verricht. Dit brengt met zich mee dat aan het beginsel van minimale gegevensverwerking wordt voldaan.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Respondent gaf aan dat zij, bij de mediaberichten die zij via LexisNexis verzamelt, uitgaat van de juistheid van de daarin voorkomende persoonsgegevens. Eventuele rectificaties worden volgens respondent ook weergegeven in LexisNexis. Wij zijn van mening dat aan het beginsel van juistheid wordt voldaan, mits deze rectificaties structureel en tijdig worden opgemerkt en gedeeld.

Mogelijke knelpunten		Aanbevelingen
Organisatorisch		
4.	<p>Het kan voorkomen dat rectificaties niet (tijdig) worden gesignaleerd, waardoor de informatievoorziening op onjuiste of onvolledige informatie is gebaseerd.</p> <p><i>Fictief voorbeeld: op maandag verwerkt DCo een mediabericht in de Nieuwsupdate/Nieuwsbrief. Op dinsdag voert de journalist een rectificatie door. Deze rectificatie wordt niet waargenomen door DCo.</i></p>	<p>Het plaatsen van een disclaimer bij mediaberichten, waarin wordt aangegeven dat het mediabericht te allen tijde onderhevig kan zijn aan rectificaties;</p> <p>Extra aandacht besteden aan berichten met een hoge nieuwswaarde voor eventuele rectificaties.</p>

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalst, dan moeten de persoonsgegevens worden gewist.

Uit de selectielijst van het Ministerie van Defensie blijkt dat persoonsgegevens in interne communicatie-uitingen, zoals folders, nieuwsoverzichten, nieuwsbrieven

en interne aankondigingen, worden bewaard voor een periode van vijf jaren.⁶⁸ Onzes inziens vallen de Nieuwsupdate en Nieuwsbrief hier ook onder, waardoor aan het beginsel van opslagbeperking wordt voldaan.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De door DCo opgestelde Nieuwsupdate en Nieuwsbrief worden uitsluitend naar bepaalde verzendgroepen verstuurd, en gedurende zeven dagen op het intranet gepubliceerd in verband met de Auteurswet en contractuele afspraken. Hoewel de mediaberichten die in de Nieuwsupdate en Nieuwsbrief zijn opgenomen al openbaar zijn, wordt er nog steeds vertrouwelijk met de informatie omgegaan door de Nieuwsupdate en Nieuwsbrief slechts naar beperkte groepen te versturen en deze slechts gedurende een beperkte tijd op het intranet gepubliceerd te houden.

Daarnaast heeft respondent aangegeven dat voor de opslag van de Nieuwsupdate en Nieuwsbrief aansluiting wordt gezocht bij de beveiligingseisen uit het Defensie Beveiligingsbeleid. Wij zijn van mening dat hiermee aan het beginsel van integriteit en vertrouwelijkheid wordt voldaan.

113

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

De verwerking van persoonsgegevens uit reeds openbare mediaberichten in de Nieuwsupdate en Nieuwsbrief is vooralsnog niet terug te vinden in het verwerkingenregister.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
5.	De verwerking van persoonsgegevens uit reeds openbare mediaberichten in de Nieuwsupdate en Nieuwsbrief	Het opnemen van een verwerking in het verwerkingenregister.

⁶⁸ Zie volgnummer 9.7 van de Selectielijst Ministerie van Defensie vanaf (1945) 2021, versie 2.1, pagina 76.

	ontbreekt in het verwerkingenregister.	
--	--	--

Conclusie

DCo beschikt volgens ons niet over een grondslag om persoonsgegevens te verwerken bij (sociale) mediamonitoring. Dit brengt met zich mee dat deze activiteit niet op deze manier kan worden voortgezet. Voor zover Defensie erin slaagt om een grondslag te creëren, zijn wij van mening dat betrokkenen op algemene basis beter kunnen worden geïnformeerd, de verwerking van persoonsgegevens in het verwerkingenregister kan worden opgenomen en er organisatorisch gezien mogelijk nog winst te behalen valt bij het opmerken van rectificaties van mediaberichten.

Activiteit 2

Omschrijving activiteit 2

De Directie Communicatie (hierna: DCo) beantwoordt vragen die binnenkomen op de corporate sociale mediakanalen van Defensie. Deze kanalen zijn YouTube, Facebook, Instagram en Twitter. De vragen die via deze corporate sociale mediakanalen worden gesteld komen bij Defensie binnen via het programma Coosto. Hierbij worden de volgende persoonsgegevens verwerkt: (gebruikers)naam, profielfoto (voor zover deze herleidbaar is tot de persoon) en eventuele (bijzondere) persoonsgegevens die vraagsteller vrijwillig met Defensie deelt.

Daarnaast volgt Defensie via haar corporate sociale mediakanalen publieke personen, zoals politici, nieuwsredacties, commandanten, binnenlandse en buitenlandse Defensie-mogendheden en ministeries.

Het verwerken van persoonsgegevens vindt plaats om binnenkomende vragen te beantwoorden.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DCo, zoals deze uit de verschillende wet- en regelgeving blijken.

115

Algemeen organisatiebesluit Defensie 2021

Artikel 7 van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) bepaalt het volgende:

“De Directeur Communicatie is belast met:

- a. Het met inachtneming van de aanwijzingen van de Secretaris-Generaal geven van ambtelijke leiding aan de Directie Communicatie;*
- b. De woordvoering namens de politieke, ambtelijke en militaire leiding, voor zover het de verantwoordelijkheid van de Minister van Defensie betreft;*
- c. Het gevraagd en ongevraagd adviseren van de politieke, ambtelijke en militaire leiding inzake mediagevoelige aangelegenheden;*
- d. De externe, interne en arbeidsmarktcommunicatie;*
- e. Het ontwikkelen, coördineren en handhaven van integraal en uitvoerend communicatiebeleid in afstemming met de Directeur-Generaal Beleid en de Rijksvoorlichtingsdienst.”*

Wij zijn van oordeel dat het beantwoorden van publieksvragen niet expliciet voortvloeit uit artikel 7 AOD.

Toepassingsbereik AVG

Materieel toepassingsbereik

Op het moment dat iemand via één van de corporate sociale mediakanalen van Defensie een vraag stelt, komt deze vraag binnen via Coosto. Het binnenkomen van persoonsgegevens in een systeem dat DCo gebruikt is een vorm van geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens. De Algemene verordening gegevensbescherming (hierna: AVG) is daarom op grond van artikel 2 van toepassing op deze verwerking.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

De AVG is dus wel van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. In deze paragraaf lichten wij de relevante grondslagen toe.

116

Toestemming

Artikel 6 lid 1 sub a AVG bepaalt dat persoonsgegevens verwerkt mogen worden als een betrokkene hiervoor ondubbelzinnig toestemming geeft. Respondent heeft aangegeven dat het stellen van vragen en de daaronder vallende verwerking van persoonsgegevens via de corporate sociale mediakanalen van Defensie is gebaseerd op de grondslag toestemming. Mogelijk wordt de betrokkene hierover onvoldoende geïnformeerd en is er sprake van het volgende knelpunt:

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het is ons opgevallen dat er geen ondubbelzinnige, actieve handeling vooraf gaat aan het stellen van een vraag via de corporate sociale mediakanalen van Defensie. Hierdoor is het voor de betrokkene mogelijk onvoldoende duidelijk welke	Zorg dat de betrokkene wordt geïnformeerd over de verwerking. Het eisen van een actieve handeling van de betrokkene kan hiervoor een invulling zijn, bijvoorbeeld het aanvinken van een akkoordverklaring.

	persoonsgegevens voor welk doel worden verwerkt.	
--	---	--

Los van het knelpunt zijn wij van mening dat toestemming als rechtsgeldige grondslag kan fungeren voor de verwerking van persoonsgegevens in deze activiteit.

Gerechtvaardigd belang

Artikel 6 lid 1 sub f AVG bepaalt dat de verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De laatste volzin van artikel 6 lid 1 sub f AVG voegt daaraan toe dat overheidsinstanties in het kader van de uitoefening van hun taken geen beroep kunnen doen op artikel 6 lid 1 sub f AVG.

In hoofdstuk 5 van dit rapport hebben wij uiteengezet dat een beroep op het gerechtvaardigd belang door overheidsinstanties alleen mogelijk is voor typisch bedrijfsmatige handelingen van die overheidsinstanties. Wij zijn van mening dat activiteiten met betrekking tot HR, financiën, control, marketing, communicatie, inkoop en beveiliging typische bedrijfsmatige handelingen kunnen zijn voor overheidsinstanties.

117

Het beantwoorden van publieksvragen is een activiteit die betrekking heeft op communicatie. Wij zijn van mening dat het verwerken van persoonsgegevens bij het beantwoorden van publieksvragen noodzakelijk is om publieksvragen effectief te kunnen beantwoorden. Met de verwerking van persoonsgegevens wordt gewaarborgd dat de juiste persoon een passend antwoord ontvangt.

Artikel 6 lid 1 sub f AVG vereist naast een gerechtvaardigd belang ook nog een belangenafweging. Het is aan DCo om deze belangenafweging te maken en vast te leggen.

Wij zijn van mening dat DCo voor het verwerken van de persoonsgegevens in Coosto mogelijk ook een beroep kan doen op het gerechtvaardigde belang. Het staat verwerkingsverantwoordelijken namelijk vrij om gebruik te maken van systemen die het beantwoorden van publieksvragen efficiënter maakt. Wij zijn van mening dat Coosto een dergelijk systeem is.

Voor zover DCo ook bijzondere persoonsgegevens verwerkt die betrokkene zelf in haar vraagstelling deelt, kan DCo voor de verwerking daarvan mogelijk gebruik maken van de doorbrekingsgrond uit artikel 9 lid 2 sub a AVG. Uit deze

bepaling blijkt dat het verbod om bijzondere persoonsgegevens te verwerken niet geldt voor zover de betrokkene uitdrukkelijk heeft ingestemd met het delen van die bijzondere persoonsgegevens. Vereiste hierbij is wel dat de toestemming van betrokkene om die persoonsgegevens te delen voldoet aan de vereisten uit artikel 7 AVG.

Concluderend merken wij op dat DCo mogelijk een succesvol beroep kan doen op artikel 6 lid 1 sub f AVG, mits aan de vereisten wordt voldaan. DCo moet onder andere de vereiste belangenafweging maken en deze moet in het voordeel van DCo uitvallen.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
2.	De vereiste belangenafweging voor een succesvol beroep op het gerechtvaardigd belang uit artikel 6 lid 1 sub f AVG is niet uitgevoerd.	Het uitvoeren van de vereiste belangenafweging.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

In de privacyverklaring op de website van Defensie staat het volgende: “Wij gebruiken uw persoonsgegevens op Defensie.nl voor afhandeling van vragen, klachten en verzoeken (inclusief inzagerecht).” Het openbare AVG-verwerkingenregister van Defensie voegt hieraan toe dat in het kader van het afhandelen van vragen, klachten en verzoeken (inclusief inzagerecht) de volgende persoonsgegevens worden verwerkt: gewone persoonsgegevens, te weten voorletters, voornaam, voorvoegsels, achternaam en contactgegevens (e-mail en/of adres, telefoonnummer).⁴

Hoewel de aard van de persoonsgegevens en het doel van de verwerking helder en transparant worden weergegeven, blijkt niet uit de privacyverklaring, noch uit het verwerkingenregister dat deze verwerking van persoonsgegevens ook betrekking heeft op vragen die worden gesteld via de corporate sociale mediakanalen. Zowel de privacyverklaring als het verwerkingenregister spreken namelijk uitsluitend over de verwerking van persoonsgegevens via de

internetsite defensie.nl. Wij zijn van mening dat daarmee niet volledig aan het beginsel van behoorlijkheid en transparantie wordt voldaan.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
3.	Het is onvoldoende duidelijk dat de privacyverklaring ook betrekking heeft op het afhandelen van vragen, klachten en verzoeken (inclusief inzagerecht) die binnenkomen op de corporate (sociale) mediakanalen van Defensie.	Het toevoegen van nieuwe passages in de privacyverklaring of het aanpassen van de huidige privacyverklaring met betrekking tot de verwerking van persoonsgegevens in relatie tot het afhandelen van vragen, klachten en verzoeken (inclusief inzagerecht) die binnenkomen op de corporate (sociale) mediakanalen van Defensie.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

119

De taken en communicatiedoeleinden van DCo zijn neergelegd in het interne beleidsstuk '*Corporate Visie op Communicatie*'. De communicatiedoeleinden die hieruit voortvloeien zijn:

- het communiceren met en verantwoording afleggen aan de eigen medewerkers en de samenleving;
- het bouwen aan vertrouwen van de eigen medewerkers en de Nederlandse burgers;
- het uitbouwen, behouden en creëren van de in- en extern draagvlak voor (de taken van) de krijgsmacht;
- het positioneren van Defensie als betrouwbare en aantrekkelijke werkgever;
- het positioneren van Defensie als aantrekkelijke partner voor relevante organisaties in de samenleving (bedrijfsleven, zorg, onderwijs).

Het doel van de verwerking van persoonsgegevens is het beantwoorden van vragen die worden gesteld via de corporate sociale mediakanalen van Defensie. Dit doel is ook vastgelegd in het interne beleidsstuk '*Corporate Visie op Communicatie*' als het communiceren met en verantwoording afleggen aan de eigen medewerkers en de samenleving. Het verwerken van persoonsgegevens is hierbij noodzakelijk om contact te onderhouden met de

vraagsteller en om het beoogde doel te realiseren. Wij zijn van mening dat hiermee aan het beginsel van doelbinding wordt voldaan.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Respondent gaf aan dat uitsluitend de persoonsgegevens worden verwerkt die vraagsteller met DCo deelt. Dit brengt met zich mee dat DCo ook bijzondere persoonsgegevens verwerkt, wanneer vraagsteller deze gegevens deelt.

Om te voorkomen dat vraagstellers te veel persoonsgegevens delen of persoonsgegevens delen die niet relevant zijn voor de verdere beantwoording van de vraag hanteert DCo een disclaimer op bepaalde corporate sociale mediakanalen. In de disclaimer staat dat vraagsteller geen privégegevens moet delen bij het stellen van de vraag via sociale media. Onduidelijk is of deze disclaimer bij alle corporate sociale mediakanalen wordt gehanteerd. Wij zijn van mening dat hiermee nog niet volledig aan het beginsel van minimale gegevensverwerking wordt voldaan.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
4.	Het verwerken van persoonsgegevens die niet relevant zijn voor de beantwoording van de gestelde vraag en bijvoorbeeld uit de vraagstelling van de betrokkene voortvloeien.	Het plaatsen van een disclaimer op de corporate sociale mediakanalen, waarin staat dat vraagsteller geen irrelevante (bijzondere) persoonsgegevens moet verstrekken.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Gelet op het feit dat de door DCo verwerkte persoonsgegevens door betrokkene zelf worden verstrekt, mag DCo uitgaan van de juistheid van die persoonsgegevens. Wij zijn van mening dat hiermee aan het beginsel van juistheid wordt voldaan.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalst, dan moeten de persoonsgegevens worden gewist.

Uit de selectielijst van het Ministerie van Defensie blijkt dat persoonsgegevens in uitingen op sociale media, in het kader van publieksvoorlichting, worden bewaard voor een periode van vijf jaren.⁵ Persoonsgegevens die worden verwerkt in het kader van het afhandelen van burgerbrieven, Wob-verzoeken en verzoeken om informatie door de Ombudsman en andere overheden, worden bewaard voor een periode van tien jaren.⁶ In de toelichting staat het volgende vermeld: *“Het reageren op acties van burgerorganisaties, particuliere instellingen en particulieren.”*

Uit de selectielijst kan niet worden afgeleid of het beantwoorden van vragen van burgers via sociale media valt onder 'publieksvoorlichting' of 'het reageren op [...] particulieren', waarvoor een bewaartermijn van vijf, respectievelijk tien jaren geldt. Wij zijn van mening dat dit nog verder geconcretiseerd kan worden om aan het beginsel van opslagbeperking te voldoen.

Daarnaast heeft respondent aangegeven dat de bewaartermijnen in de praktijk mogelijk niet worden gehanteerd. Vragen en de daarbij behorende persoonsgegevens die in Coosto worden verwerkt worden niet handmatig door DCo verwijderd na verloop van de vastgestelde bewaartermijn. Wij zijn van mening dat aan het beginsel van opslagbeperking nog niet volledig wordt voldaan.

Mogelijke knelpunten		Aanbevelingen
Juridisch		
5.	Uit de selectielijst blijkt niet duidelijk onder welke categorie de persoonsgegevens vallen die worden verwerkt in het kader van binnenkomende vragen op de corporate sociale mediakanalen van Defensie.	Concretiseren onder welke categorie de persoonsgegevens vallen en verantwoorden waarom aansluiting wordt gezocht bij die bewaartermijn.

Mogelijke knelpunten		Aanbevelingen
Organisatorisch		
6.	Onduidelijk is of de bewaartermijnen uit de	Een werkinstructie opstellen ten aanzien van het verwijderen van

	selectielijsten ook daadwerkelijk worden gehanteerd.	beantwoorde vragen, zodat aan de bewaartermijnen wordt voldaan.
--	--	---

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Verwerkersovereenkomst Coosto

Respondent heeft aangegeven dat Coosto met al haar partijen een verwerkersovereenkomst sluit, waarin staat dat Coosto vertrouwelijk met persoonsgegevens omgaat. Defensie heeft ook een dergelijke verwerkersovereenkomst met Coosto gesloten. Onzes inziens biedt de verwerkersovereenkomst voldoende waarborgen voor de omgang met en beveiliging van persoonsgegevens.

Autorisatiebeleid

Dco beschikt over een project binnen Coosto, waar accounts van diverse medewerkers van Dco onder hangen. Deze personen zijn geautoriseerd om de persoonsgegevens in Coosto te raadplegen. De persoonsgegevens die door vraagsteller worden verstrekt via de corporate sociale mediakanalen zijn in beginsel echter niet relevant voor medewerkers buiten Dco, tenzij interne deskundigen moeten worden ingeschakeld om de vraag te kunnen beantwoorden. Defensie zal dus zorg moeten dragen voor een autorisatiebeleid, waaruit blijkt welke medewerkers toegang hebben tot de in Coosto verwerkte persoonsgegevens.

122

Volledigheidshalve merken wij op dat de persoonsgegevens van vraagsteller ook voor vraagsteller zelf zichtbaar zijn via het door vraagsteller gebruikte sociale mediaplatform.

Defensie Beveiligingsbeleid

Daarnaast heeft respondent aangegeven dat voor de verwerking van persoonsgegevens aansluiting wordt gezocht bij de beveiligingseisen uit het Defensie Beveiligingsbeleid. Wij zijn van mening dat hiermee aan het beginsel van integriteit en vertrouwelijkheid wordt voldaan.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

De verwerking van persoonsgegevens voor het beantwoorden van vragen die worden gesteld via de corporate sociale mediakanalen is gedeeltelijk terug te vinden in het verwerkingenregister. Dit wordt hieronder nader toegelicht.

Burgerbrieven (M1686)

Uit deze verwerking blijkt dat er persoonsgegevens worden verwerkt bij burgerbrieven voor een tijdige beantwoording van vragen van burgers. Uit deze verwerking blijkt ook dat het beantwoorden van een burgerbrief niet mogelijk is zonder correspondentiegegevens.

Uitvoeren communicatiebeleid, sociale media en monitoring (M1739)

Hoewel respondent deze verwerking heeft opgegeven, is deze nog niet openbaar raadpleegbaar in het verwerkingenregister van Defensie.

Internetsite www.defensie.nl (M2302)

Uit deze verwerking blijkt dat er persoonsgegevens worden verwerkt via de internetsite www.defensie.nl voor het afhandelen van vragen, klachten en verzoeken. De persoonsgegevens worden bewaard totdat de vraag, de klacht of het verzoek is beantwoord. Zonder persoonsgegevens is het niet mogelijk om contact te onderhouden met de aanvrager/verzoeker en het beoogde doel te realiseren.

Wob-verzoeken (M2311)

Uit deze verwerking blijkt dat er persoonsgegevens worden verwerkt voor de behandeling, de afdoening en archivering van verzoeken op grond van de Wet openbaarheid van bestuur, de communicatie met betrokkenen, het bijhouden van een overzicht van de verzonden informatie of besluiten en de daarover gemaakte afspraken en het doen behandelen van geschillen, bezwaar- en beroepsprocedures.

Gelet op het feit dat activiteit M1739 nog niet openbaar raadpleegbaar is, zijn wij van mening dat nog niet volledig aan de verantwoordingsplicht wordt voldaan.

Mogelijke knelpunten		Aanbevelingen
Juridisch		
7.	De verwerking van persoonsgegevens in deze activiteit is nog niet expliciet terug te vinden in het verwerkingenregister van Defensie.	Het publiceren van activiteit M1739 in het verwerkingenregister van Defensie.

Conclusie

Wij zijn van mening dat DCo bij het verwerken van persoonsgegevens mogelijk een succesvol beroep kan doen op het gerechtvaardigde belang in de zin van artikel 6 lid 1 sub f AVG. Hierbij is het wel vereist dat DCo de vereiste belangenafweging maakt en deze in het voordeel uitvalt van DCo. Daarnaast kan er bij deze activiteit meer aandacht worden besteed aan het informeren van betrokkenen door de privacyverklaring te concretiseren en kan er meer aandacht worden besteed aan de bewaartermijnen door de selectielijst te concretiseren en de daarin opgenomen bewaartermijnen ook daadwerkelijk te hanteren.

Activiteit 3

Omschrijving activiteit 3

Defensie Cyber Commando (hierna: DCC) ontwikkelt een algoritme dat netwerken en verbanden in kaart kan brengen. Dit wordt Social Network Analysis (hierna: SNA) genoemd. Het doel is om door middel van de Artificial Intelligence (hierna: AI) sociale structuren in kaart te brengen en uitlatingen te analyseren om zo groepen – en belangrijke personen binnen die groepen en hun status – te identificeren. Daarbij ligt de focus op het in beeld brengen van actoren die bepaalde boodschappen uitzenden. Ook stelt de AI vast hoe er binnen het netwerk op de uitlating wordt gereageerd.

Een algoritme is in principe niet meer dan een automatisch stappenplan dat door de computer wordt doorlopen. Een AI is een systeem dat is gebaseerd op machine learning. Dat wil zeggen dat een AI wordt getraind op basis van algoritmes en grote hoeveelheden voorbeelddata. Hierdoor kan de computer uiteindelijk zelfstandig taken uitvoeren.⁶⁹

Naast SNA bestaat de wens binnen DCC om ook een capaciteit te ontwikkelen voor Social Network Influencing (hierna: SNI). Dit houdt in dat de personen die binnen een netwerk veel invloed uitoefenen worden beïnvloed. Het doel is dat de personen die veel invloed uitoefenen hierdoor andere informatie verspreiden binnen hun netwerk/omgeving. De te ontwikkelen capaciteit is bedoeld ter ondersteuning van militaire operaties en/of voor bijstand aan de civiele autoriteiten (politie op grond van art. 58 Politiewet/andere autoriteiten onder de Regeling Militaire Steunverlening in het Openbaar Belang (hierna: MSOB). Vanuit Defensie is besloten dat het beïnvloeden van externen buiten de scope van dit onderzoek valt. Daarom is SNI niet verder uitgewerkt.

125

De enige mogelijke behoefte om – in het kader van dit project – zelfstandig persoonsgegevens te verwerken, had zich kunnen opdienen tijdens de ontwikkelfase van de AI. De ontwikkeling van de AI vereist namelijk input in de vorm van datasets bestaande uit uitlatingen (in wat voor vorm dan ook) door individuen/groeperingen, bijvoorbeeld op sociale media of internetfora.

Aangezien de krijgsmacht geen zelfstandige bevoegdheid heeft om persoonsgegevens te verwerken, onderzocht het projectteam de volgende alternatieven:

⁶⁹ Voor meer informatie over algoritmes en AI zie: *Toezicht op AI & Algoritmes (Autoriteit Persoonsgegevens)*. Dit document is raadpleegbaar via de website van de Autoriteit Persoonsgegevens.

1. Aankopen van geanonimiseerde of fictieve datasets, bijvoorbeeld van een derde partij die over grote datasets beschikt. Aandachtspunten daarbij zijn de volgende:
 - a. het is de vraag of datasets daadwerkelijk geen persoonsgegevens bevatten (een combinatie van geanonimiseerde of gepseudonimiseerde gegevens zou onder omstandigheden alsnog gegevens kunnen bevatten die te herleiden zijn naar een natuurlijk persoon);
 - b. bovendien is het moeilijk om na te gaan of de aangekochte gegevens rechtmatig zijn verkregen.
2. Zelf creëren van fictieve datasets. Uitdaging hierbij is dat de te creëren datasets voldoende complex en grootschalig moeten zijn om de AI te kunnen trainen. DCC heeft voor deze insteek gekozen.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DCC, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub b van het AOD bepaalt dat het Ministerie van Defensie de Commandant der Strijdkrachten als verantwoordelijke kent.

Artikel 3 AOD bepaalt over de Commandant der Strijdkrachten het volgende:

“De Commandant der Strijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Secretaris-Generaal geven van ambtelijke leiding aan de Defensiestaf;*
- b. de taak van de militaire adviseur van de Minister van Defensie;*
- c. het met inachtneming van de aanwijzingen van de Minister van Defensie aansturen van de voorbereidingen, uitvoering en evaluatie van alle operaties, alsmede het zorg dragen voor de implementatie van de verbetermaatregelen naar aanleiding van de evaluaties van operaties;*
- d. het aansturen van de gereedstelling van de krijgsmacht;*

- e. *het aansturen van de krijgsmacht, te weten het Commando Zeestrijdkrachten, het Commando Landstrijdkrachten, het Commando Luchstrijdkrachten, het Defensie Cybercommando en het (NLD) Special Operations Command alsmede het aansturen van de Defensie Materieel Organisatie en het Defensie Ondersteuningscommando;*
- f. *het aansturen van de inzet van het Commando Koninklijke Marechaussee voor zover het de verantwoordelijkheid van de Minister van Defensie betreft;*
- g. *het bijdragen aan beleidsontwikkeling en integraal toetsen van beleid op uitvoerbaarheid;*
- h. *organisatieontwikkeling (zowel het operationaliseren van beleid (top down) als integraal advies over bottom-up initiatieven) van de krijgsmacht inclusief het opstellen van behoeftestellingen voor militaire capaciteiten;*
- i. *de bi- en multilaterale militaire samenwerking binnen de kaders van het vastgestelde internationaal beleid en de samenhang en eenduidigheid van de inbreng in internationaal militair verband."*

Subtaakbesluit

Artikel 26 AOD bepaalt dat de Commandant der Strijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

127

Subtaakbesluit Commando Landstrijdkrachten 2015

Artikel 2 lid 4 sub j subtaakbesluit bepaalt dat de Commando Landstrijdkrachten bestaat uit het Defensie Cyber Commando. Artikel 17 van het subtaakbesluit kent de volgende taken toe aan het Defensie Cyber Commando:

"Het Defensie Cyber Commando Land staat onder leiding van de Commandant Cyber Commando die is belast met:

- a. *het, met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Landstrijdkrachten, geven van de ambtelijke leiding aan het Defensie Cyber Commando;*
- b. *het operationeel gereed stellen van eenheden (teams van cyberadviseurs/-operators) en het in stand houden van de gereedheidstatus;*
- c. *het formeren, inzet gereed stellen en bijdragen aan de instandhouding van operationeel gereede respectievelijk ingezette eenheden (teams van cyberadviseurs/-operators);*
- d. *het uitvoeren van nazorg en recuperatie van operationeel ingezette eenheden (teams van cyberadviseurs/-operators);*
- e. *het zorg dragen voor de cyber kennisontwikkeling, -borging en -verspreiding binnen Defensie.*

- f. *het ontwikkelen en onderhouden van kennisproducten/doctrines op het gebied van cyber;*
- g. *het ontwikkelen en verzorgen van opleidingen op het gebied van cyber;*
- h. *het leveren van hoogwaardige (technische) middelen en mensen, om in het cyberdomein offensief te kunnen optreden;*
- i. *het uitvoeren van militaire bijstand en militaire steunverlening;*
- j. *het leveren van een bijdrage aan de informatiebehoefte van de Commandant Landstrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid."*

Op grond van het subtaakbesluit (in het bijzonder artikel 17 sub f en h) is het bouwen van een AI als taak van DCC te kwalificeren.

Toepassingsbereik AVG

De AVG is van toepassing als de activiteit binnen het materieel en territoriaal toepassingsgebied van de AVG valt.

Materieel toepassingsgebied

Bij de ontwikkeling van de AI verwerkt DCC op dit moment geen persoonsgegevens. De activiteit valt daarom niet binnen het materieel toepassingsbereik van de AVG.

128

Territoriaal toepassingsgebied

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland valt een eventuele verwerking van persoonsgegevens op grond van artikel 3 AVG wel binnen het territoriaal toepassingsgebied van de AVG.

DCC verwerkt geen persoonsgegevens. De AVG is dus niet van toepassing op de ontwikkeling van de AI. Mocht de AI – wanneer deze eenmaal ontwikkeld is – ooit worden ingezet in het kader van een militaire operatie, dan valt dit wel onder het toepassingsbereik van de AVG, maar dan is DCC daar niet voor verantwoordelijk. Als de AI zou worden ingezet ter ondersteuning van de politie bij de handhaving van de strafrechtelijke rechtsorde, dan zou dit geschieden onder aansturing, gezag en verantwoordelijkheid van de Minister van Justitie en Veiligheid. De verantwoordelijkheid voor een eventuele verwerking van persoonsgegevens zou dan ook bij die Minister liggen en niet bij de Minister van Defensie. Mocht in de toekomst blijken dat de wens of noodzaak alsnog bestaat om de AI te trainen en up-to-date te houden met persoonsgegevens dan ontbreekt hiervoor momenteel een grondslag.

Toetsing activiteit

Deze activiteit is niet getoetst aan de beginselen uit artikel 5 AVG om de volgende redenen:

- Bij de ontwikkeling van de AI worden geen persoonsgegevens verwerkt;
- DCC is de ontwikkelaar en dus niet de (eind)gebruiker van de AI. De gebruiker geeft uiteindelijk invulling aan de beginselen van artikel 5 AVG. Denk hierbij aan de rechtmatigheid voor het inzetten van de AI. Dit neemt niet weg dat DCC wél mee kan denken bij de beginselen privacy by design en privacy by default. Hierbij is het mogelijk om de uitgangspunten van de Aanwijzing Kaders Data (Science) projecten, kenmerk DGB-CIO-101 te hanteren.

Conclusie

Bij de ontwikkeling van de AI worden geen persoonsgegevens verwerkt. Om de AI toch te kunnen ontwikkelen, is gezocht naar fictieve of volledig anonieme datasets en tegelijkertijd wordt de mogelijkheid onderzocht om zelf (fictieve) datasets te creëren. Inmiddels is besloten om zelf datasets te creëren en verder af te zien van het zoeken naar beschikbare datasets. Let op: mocht in de toekomst blijken dat de wens bestaat om de AI te trainen met persoonsgegevens dan ontbreekt hiervoor momenteel een grondslag. Omdat er momenteel geen persoonsgegevens worden verwerkt krijgt deze activiteit de kleur groen.

Activiteit 4

Omschrijving activiteit 4

Het Defensie Cyber Commando (hierna: DCC) houdt zich bezig met en zet zich in voor de digitale veiligheid van de hele Defensieorganisatie en haar partners.

Op grond van artikel 57 Politiewet (hierna: Pw) kan de Koninklijke Marechaussee (hierna: KMar) bijstand verlenen aan de politie. Dit is het geval als de benodigde capaciteit bij de politie ontbreekt. Artikel 58 Pw bepaalt dat in 'bijzondere gevallen' ook andere onderdelen van de krijgsmacht bijstand kunnen verlenen aan de politie. Een bijzonder geval wil zeggen als KMar niet in staat of in de gelegenheid is om de verzochte capaciteit te leveren. Na een verzoek om bijstand door de Minister van Justitie en Veiligheid (hierna: MinJ&V) bepaalt de Minister van Defensie of en hoe deze bijstand wordt verleend. Bij de uitvoering van de bijstandstaken staat het krijgsmachtpersoneel onder het gezag van de Officier van Justitie (hierna: OvJ). De OvJ is ook verantwoordelijk voor de werkzaamheden die het personeel uitvoert.⁷⁰ Defensie stelt dus van tevoren de voorwaarden vast voor de militaire bijstand, maar is inhoudelijk niet betrokken bij de uit te voeren werkzaamheden.

Met enige regelmaat ontvangt DCC verzoeken voor militaire bijstand van civiele autoriteiten. In dat kader zet DCC, naast regulier militair personeel, soms ook reservepersoneel in uit de bij DCC gecentraliseerde pool van "cyberreservisten". Dit zijn reservisten met specifieke ICT-expertise. Reservisten zijn personen die normaal gesproken werkzaam zijn buiten Defensie en op vrijwillige basis worden opgeroepen door Defensie om tijdelijk bepaalde werkzaamheden te verrichten. Tijdens de oproep/uitvoering van werkzaamheden hebben deze reservisten de status van militair.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DCC, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de

⁷⁰ De organisatie die bijstand levert staat bij de uitvoering van de bijstand onder hetzelfde gezag als de organisatie die bijstand ontvangt, MvT Politiewet 2012, p. 6.

internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub b van het AOD bepaalt dat het Ministerie van Defensie de Commandant der Strijdkrachten als verantwoordelijke kent.

Artikel 3 AOD bepaalt over de Commandant der Strijdkrachten het volgende:

“De Commandant der Strijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Secretaris-Generaal geven van ambtelijke leiding aan de Defensiestaf;*
- b. de taak van de militaire adviseur van de Minister van Defensie;*
- c. het met inachtneming van de aanwijzingen van de Minister van Defensie aansturen van de voorbereidingen, uitvoering en evaluatie van alle operaties, alsmede het zorg dragen voor de implementatie van de verbetermaatregelen naar aanleiding van de evaluaties van operaties;*
- d. het aansturen van de gereedstelling van de krijgsmacht;*
- e. het aansturen van de krijgsmacht, te weten het Commando Zeestrijdkrachten, het Commando Landstrijdkrachten, het Commando Luchstrijdkrachten, het Defensie Cybercommando en het (NLD) Special Operations Command alsmede het aansturen van de Defensie Materieel Organisatie en het Defensie Ondersteuningscommando;*
- f. het aansturen van de inzet van het Commando Koninklijke Marechaussee voor zover het de verantwoordelijkheid van de Minister van Defensie betreft;*
- g. het bijdragen aan beleidsontwikkeling en integraal toetsen van beleid op uitvoerbaarheid;*
- h. organisatieontwikkeling (zowel het operationaliseren van beleid (top down) als integraal advies over bottom-up initiatieven) van de krijgsmacht inclusief het opstellen van behoeftestellingen voor militaire capaciteiten;*
- i. de bi- en multilaterale militaire samenwerking binnen de kaders van het vastgestelde internationaal beleid en de samenhang en eenduidigheid van de inbreng in internationaal militair verband.”*

131

Subtaakbesluit

Artikel 26 AOD bepaalt dat de Commandant der Strijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Landstrijdkrachten 2015

Artikel 2 lid 4 sub j van het Subtaakbesluit Commando Landstrijdkrachten 2015 (hierna: subtaakbesluit) bepaalt dat de Commando Landstrijdkrachten bestaat uit het Defensie Cyber Commando. Artikel 17 van het subtaakbesluit kent de volgende taken toe aan het Defensie Cyber Commando:

"Het Defensie Cyber Commando Land staat onder leiding van de Commandant Cyber Commando die is belast met:

- a. het, met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Landstrijdkrachten, geven van de ambtelijke leiding aan het Defensie Cyber Commando;*
- b. het operationeel gereed stellen van eenheden (teams van cyberadviseurs/-operators) en het in stand houden van de gereedheidstatus;*
- c. het formeren, inzet gereed stellen en bijdragen aan de instandhouding van operationeel gereede respectievelijk ingezette eenheden (teams van cyberadviseurs/-operators);*
- d. het uitvoeren van nazorg en recuperatie van operationeel ingezette eenheden (teams van cyberadviseurs/-operators);*
- e. het zorg dragen voor de cyber kennisontwikkeling, -borging en -verspreiding binnen Defensie.*
- f. het ontwikkelen en onderhouden van kennisproducten/doctrines op het gebied van cyber;*
- g. het ontwikkelen en verzorgen van opleidingen op het gebied van cyber;*
- h. het leveren van hoogwaardige (technische) middelen en mensen, om in het cyberdomein offensief te kunnen optreden;*
- i. het uitvoeren van militaire bijstand en militaire steunverlening;*
- j. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Landstrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid."*

132

Op grond van het subtaakbesluit (in het bijzonder artikel 17 sub i) is het inzetten van cyberreservisten in het kader van militaire bijstand en MSOB aan te merken als taak van DCC.

Toepassingsbereik AVG

Materieel & territoriaal toepassingsbereik

Vanwege de aard van militaire bijstand (gezag en verantwoordelijkheid bij MinJ&V) is Defensie zelf niet verantwoordelijk voor de verwerking van persoonsgegevens. Om deze scheiding van verantwoordelijkheden te waarborgen en te voorkomen dat in het kader van militaire bijstand verwerkte persoonsgegevens op enige wijze bij Defensie terechtkomen, voorziet de politie de cyberreservisten van eigen accounts op de politie-netwerken.

Cyberreservisten ontwikkelen ook software en tools voor de politie. Deze software en tools blijven wel altijd 'eigendom' van Defensie. Ook worden de software en tools eventueel ontdaan van persoonsgegevens voordat zij 'terugkomen' naar het defensienetwerk.

DCC verwerkt geen persoonsgegevens (behoudens NAW-gegevens van defensiepersoneel) in het kader van militaire bijstand.⁷¹ De cyberreservisten verwerken in sommige gevallen wel persoonsgegevens, bijvoorbeeld in het kader van ondersteuning van een strafrechtelijk onderzoek. Dit valt onder gezag en verantwoordelijkheid van een OvJ en dus de MinJ&V. DCC (of de minister van Defensie) is dus in het kader van militaire bijstand nooit aan te merken als verwerkingsverantwoordelijke. Om die reden worden de beginselen van artikel 5 AVG in dit rapport niet getoetst.

Mogelijk knelpunt

Hoewel de activiteit zelf geen verwerking van persoonsgegevens is onder verantwoordelijkheid van DCC, verwerken cyberreservisten wel persoonsgegevens bij inzet of militaire bijstand. Er is mogelijk wel één knelpunt:

Mogelijke knelpunt		Aanbeveling
Organisatorisch		
1.	Cyberreservisten kunnen mogelijk baat hebben bij (meer, in tegenstelling tot ad hoc) structurele kennis van privacy.	Onlangs is er voor het eerst een training gegeven aan enkele cyberreservisten. Het is raadzaam om structureel privacy trainingen te verzorgen voor de cyberreservisten. Zeker bij de werkzaamheden van cyberreservisten is het van belang dat zij op de hoogte zijn van de geldende wet- en regelgeving, zodat cyberreservisten weten wat ze wel en niet mogen doen. Door structureel trainingen te geven wordt ook de bewustwording vergroot. Momenteel worden cyberreservisten ad hoc gebriefd over wat zij wel en niet mogen doen als er persoonsgegevens worden verwerkt bij een project waarbij zij worden ingezet. Toch is het

⁷¹ Persoonsgegevens (NAW-gegevens) worden conform de selectielijst bewaard en vernietigd. Zie volgnnummer 14.2 van de Selectielijst Ministerie van Defensie vanaf (1945) 2021, versie 2.1, pagina 97.

		raadzaam om periodiek privacy trainingen te geven.
--	--	--

Conclusie

De activiteit kan doorgaan op de huidige manier. DCC verwerkt ten behoeve van deze activiteit geen persoonsgegevens en er is geen indicatie dat dit in de nabije toekomst verandert. Het is wel een aanbeveling om te zorgen dat de cyberreservisten over voldoende privacy kennis beschikken. De activiteit kan op de huidige manier doorgang vinden, daarom krijgt deze activiteit de kleur groen.

Activiteit 5A

Omschrijving activiteit 5A

Met enige regelmaat ontvangt Defensie verzoeken voor militaire bijstand of militaire steunverlening in het openbaar belang (hierna: MSOB) van civiele autoriteiten. Deze militaire inzet/bijstand door Defensie bij Chemische, Biologische, Radioactieve en Nucleaire (hierna: CBRN) incidenten of specialistische zoekhulp (Advanced Search Teams) vindt plaats via de officiële route volgens de Wet veiligheidsregio's, de Politiewet 2012 en/of MSOB.

Deze activiteit gaat in op ondersteuning door Defensie middels eenheden of teams met specifieke expertise, onder andere door:

- **CBRN Respons Eenheid (hierna: CBRN RE).** De CBRN RE staat dag en nacht paraat om civiele hulpdiensten bij eventuele CBRN dreigingen en incidenten advies en ondersteuning te bieden. De CBRN RE detecteert, identificeert en ontsmet met specialistische apparatuur. Waar nodig wordt ook geadviseerd over mogelijke neutralisatie van stoffen. Dit vindt plaats in het fysieke domein. De CBRN RE verzamelt data van en over stoffen om hier aansluitend een advies op te geven of mogelijk actie op te plannen. Hierbij worden geen persoonsgegevens verwerkt. Er vindt enkel een registratie van locatie en tijdstip plaats, maar dit is niet te herleiden naar een natuurlijk persoon.
- **Advanced Search Teams (hierna: AST).** Dit zijn zoekteams met specialisten en apparatuur van Defensie bestaande uit militairen met kennis en ervaring opgedaan tijdens missies en operaties in het buitenland – en Nederland zelf – over het onderkennen en doorzoeken van het gehele fysieke domein. Hierbij worden geen persoonsgegevens verwerkt, het gaat enkel om lezen met sensoren. De civiele autoriteit aan wie bijstand of ondersteuning wordt verleend (veelal justitie) bepaalt waar het AST naar zoekt. Deze specialisten komen voort uit alle krijgsmachtdelen en zijn dus niet specifiek gelieerd aan de Genie. Voor het samenstellen van een AST wordt gecoördineerd tussen de Directie Operaties en het uitvoerende krijgsmachtonderdeel.

135

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van de Genie, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht. Ook uit artikel 97 Gw kan geen wettelijke verplichting of taak van algemeen belang of openbaar gezag worden afgeleid.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub I van het AOD bepaalt dat het Ministerie van Defensie de Commandant Landstrijdkrachten als verantwoordelijke kent.

Artikel 13 AOD bepaalt het volgende:

“De Commandant Landstrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Landstrijdkrachten;*
- b. De gereedstelling en instandhouding van de landstrijdkrachten;*
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. Het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Landstrijdkrachten;*
- e. De advisering op het gebied van militair landoptreden.”*

136

Subtaakbesluit Commando Landstrijdkrachten 2015

Artikel 26 AOD bepaalt dat de Commandant Landstrijdkrachten op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Het Subtaakbesluit Commando Landstrijdkrachten 2015 (hierna: subtaakbesluit) artikel 14, Het Opleidings- en Trainingscommando kent de volgende taken toe met betrekking tot training en opleiding:

“Het Opleidings- en Trainingscommando staat onder leiding van de Commandant Opleidings- en Trainingscommando die is belast met:

- a. Het, met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Landstrijdkrachten, geven van de ambtelijke leiding aan het Opleidings- en Trainingscommando;*
- b. Het operationeel gereed stellen van CBRN respons eenheid en het in stand houden van de gereedheidstatus;*

- c. *Het formeren, inzet gereed stellen en bijdragen aan de instandhouding van operationeel gereede respectievelijk ingezette CBRN respons eenheid;*
- d. *Het uitvoeren van nazorg en recuperatie van operationeel ingezette CBRN respons eenheid;*
- e. *Het ontwikkelen en verzorgen van in-, door- en uitstroomopleidingen;*
- f. *Het bieden van trainingsondersteuning op niveau 2 t/m 6;*
- g. *Het ontwikkelen en onderhouden van kennisproducten/doctrines op het gebied van landoptreden;*
- h. *Het coördineren van externe dienstverlening op gebied van opleiding en training en het toezien op conforme uitvoering;*
- i. *Het uitvoeren van militaire bijstand en militaire steunverlening;*
- j. *Het leveren van een bijdrage aan de informatiebehoefte van de Commandant Landstrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid."*

De activiteiten van de CBRN RE zijn voor zover het is gericht het uitvoeren van militaire bijstand en steunverlening terug te voeren op het subtaakbesluit, in het bijzonder artikel 14 sub i. Bij deze sub activiteit zijn de activiteiten van het AST altijd gericht op het uitvoeren van militaire bijstand en MSOB.

137

Vanwege de samenstelling van het AST, namelijk specialisten afkomstig van alle krijgsmachtdelen (waaronder genisten), worden hier de specifieke subtaakbesluiten waarop deze taak is gestoeld niet afzonderlijk benoemd.

Toepassingsbereik AVG

Materieel toepassingsbereik

Vanwege de aard van militaire bijstand (gezag en verantwoordelijkheid bij MinJ&V) is Defensie zelf niet verantwoordelijk voor de verwerking van persoonsgegevens. Als de activiteiten namelijk plaatsvinden op grond van militaire bijstand of MSOB, treedt Defensie op als verwerker namens de civiele autoriteit aan wie de bijstand of steunverlening wordt gegeven. Defensie heeft in dat geval geen eigen verwerkingsgrondslag, maar oefent alleen bevoegdheden van de ondersteunde civiele autoriteit uit. De civiele autoriteit is voor deze gevallen verwerkingsverantwoordelijke.⁷²

De Genie verwerkt doorgaans geen persoonsgegevens (behoudens NAW-gegevens van Defensiepersoneel) in het kader van militaire bijstand of MSOB onder eigen verantwoordelijkheid.⁷³ AST's verwerken in sommige gevallen wel persoonsgegevens, bijvoorbeeld in het kader van ondersteuning van een

⁷² DJZ april 2021, Algemene juridische kaders voor activiteiten in de informatieomgeving, p. 6.

⁷³ Persoonsgegevens (NAW-gegevens) worden conform de selectielijst bewaard en vernietigd. Zie volgnummer 14.2 van de Selectielijst Ministerie van Defensie vanaf (1945) 2021, versie 2.1, pagina 97.

strafrechtelijk onderzoek. Dit valt onder verantwoordelijkheid van de civiele autoriteit. De civiele autoriteit bepaalt waar naar wordt gezocht en bepaalt daarmee het doel en de middelen van de verwerking. Defensie is dus in het kader van militaire bijstand niet aan te merken als verwerkingsverantwoordelijke. Een verdere beoordeling of toetsing aan de AVG (artikel 5 AVG in het bijzonder) voor wat betreft het leveren van militaire steunverlening aan civiele autoriteiten blijft daarom uit.

Mogelijke knelpunten

Hoewel bij de activiteit geen persoonsgegevens worden verwerkt onder verantwoordelijkheid van de Genie zijn er enkele mogelijke knelpunten gesignaleerd. Het eerste mogelijke knelpunt ziet op de mogelijkheid om een grotere bijdrage te kunnen leveren aan de informatievoorziening van Defensie door AST's. Het tweede knelpunt ziet op de eigen veiligheid van de CBRN RE en AST's.

Mogelijk knelpunt		Aanbeveling
<i>Juridisch (grondslag)</i>		
1.	<p>De respondent heeft aangegeven dat AST's aan de hand van dataverzameling en bijbehorende analyse mogelijk een grotere bijdrage kunnen bieden. AST's zijn in staat om een variëteit aan data te verzamelen. Dit kan data zijn van:</p> <ul style="list-style-type: none"> • foto's; • artikelen waar mogelijke biometrie (sigaretten, bekens etc) op zit; • of de biometrische gegevens zelf door het verzamelen van vingerafdrukken, haar, nagels enzovoort. <p>Deze mogelijke extra bijdrage vond tijdens het onderzoek niet plaats, omdat hulpdiensten (politie) dit momenteel zelf uitvoeren. Defensie heeft dus geen zelfstandige grondslag of mandaat om persoonsgegevens</p>	<p><i>Formeel wettelijke grondslag</i></p> <p>Het is aan de wetgever om wetgeving te creëren voor overheidsorganisaties waaruit taken en bevoegdheden zijn te ontleen. Deze taken en bevoegdheden moeten daarbij voldoende duidelijk en concreet zijn om te kwalificeren als grondslag in de zin van artikel 6 lid 1 sub e AVG. Het is daarom aan de wetgever om te bepalen of het wenselijk is dat de AST's deze en/of soortgelijke activiteiten uitvoert. Wij adviseren in ieder geval om de taken en bijbehorende bevoegdheden op een heldere en voor de betrokkene duidelijke wijze vast te leggen in (formele) wetgeving waarbij de beginselen van de AVG in acht worden genomen.</p>

	te verwerken en wellicht van grotere betekenis te kunnen zijn.	
--	--	--

Mogelijk knelpunt		Aanbeveling
<i>Organisatorisch</i>		
2.	<p>De respondent geeft aan dat veiligheid van eigen personeel (CBRN RE & AST's) een mogelijk knelpunt is. De gegevens- en identiteitsbescherming van eigen Defensiepersoneel tijdens het uitvoeren van operaties in het nationale domein is mogelijk onvoldoende gewaarborgd. Het gaat namelijk om (relatief, rond de 60 Fte) kleine teams met hele specifieke kennis. Tijdens deze acties kunnen omstanders of bewoners van objecten dicht bij een AST komen. Het is daarom tijdens een ondersteuningsactie bij de politie (bijvoorbeeld gericht op het doorzoeken van een huis op verborgen ruimtes om bewijslast te vinden) lastig om anoniem te blijven.⁷⁴</p> <p>Er bestaat mogelijk een spanningsveld tussen wat eenheden willen – bescherming persoonlijke levenssfeer van personeel – en Defensie, zij wil laten zien welke specialistische kennis zij in huis heeft.⁷⁵</p>	<p>Onderzoek de mogelijkheden en wenselijkheid om bij militaire bijstand door de CBRN RE en AST's het defensiepersoneel (onzichtbaar) te laten 'mengen' met de hulpdiensten ter plaatse. Bijvoorbeeld door het dragen van hetzelfde uniform. Respondent heeft aangegeven dat hier eerder over is nagedacht, maar niet is toegepast. Om te voorkomen dat de aandacht wordt getrokken - bijvoorbeeld door het gebruik van gezichtsbedekkende attributen - lijkt dit ons een potentieel werkbare oplossing.</p>

⁷⁴ Zie ook: <https://magazines.defensie.nl/defensiekrant/2015/07/op-pad-met-het-zoekteam-van-de-landmacht>.

⁷⁵ Zie bijvoorbeeld de volgende nieuwsberichten: <https://magazines.defensie.nl/defensiekrant/2015/07/op-pad-met-het-zoekteam-van-de-landmacht>; en: Specialistische zoekteams Defensie vinden bewijsmateriaal in drugszaak | Nieuwsbericht | Defensie.nl.

Conclusie

Het leveren van militaire bijstand/MSOB aan civiele autoriteiten die de CBRN RE van de Genie en AST's uitvoeren kan in de huidige vorm doorgaan. De verwerking van persoonsgegevens vindt plaats onder verantwoordelijkheid van de civiele autoriteit. Er zijn mogelijke knelpunten gesignaleerd bij zowel militaire bijstand/MSOB. Deze blokkeren de doorgang van de het leveren van militaire bijstand/MSOB echter niet direct. Daarom krijgt deze activiteit de kleur groen.

N.B.

Hierna wordt kort afgesloten met enkele ontwikkelingen die gaande zijn en met de respondent zijn besproken. Deze ontwikkelingen beïnvloeden de kleurcodering van de activiteit echter niet.

Overige besproken ontwikkelingen

Volgens de respondent zijn er bij Genie nog enkele ontwikkelingen gaande die gelet op de Quicksan buiten de scope van het onderzoek vallen. Vanwege de signaleringsfunctie van dit onderzoek om mogelijke knelpunten met de AVG te benoemen beschrijven we deze ontwikkelingen echter wel. Deze ontwikkelingen hebben vanwege het achterblijven van een integrale toetsing geen invloed op de kleurcodering van de activiteit. We geven enkel verkorte aanbevelingen mee om handvatten te geven voor een vervolgonderzoek naar de deze nog verder uit te diepen ontwikkelingen. Het gaat om de volgende ontwikkelingen:

140

- Artificial Intelligence (hierna: AI) gebruiken om zoveel mogelijk informatie (online) te verzamelen over Improvised Explosive Devices (hierna: IED) of explosive threat in het algemeen. Dit met als doel de veiligheid van personeel garanderen. Het is gericht op het aan de voorkant aangrijpen van het netwerk en heel sturend verzamelen en analyseren van het web. Een IED vernietigen kost veel geld vanwege de concentratie van middelen en mensen. De werkwijze met een AI is erop gericht om de voorspelling van IED dreiging aan de voorkant zo betrouwbaar mogelijk te maken. Het is niet de bedoeling om specifiek gericht op natuurlijke personen persoonsgegevens te verwerken. Er wordt bijvoorbeeld enkel gesproken over een 'noordoostelijke cel'. Soms wordt een pseudoniem verwerkt indien iemand op een openbaar internetforum informatie plaatst onder een andere dan zijn eigen naam. Er is geen formele steunaanvraag (militaire bijstand en/of MSOB) gedaan waaronder of waarvoor deze AI wordt ontwikkeld. De ontwikkeling staat op dit moment nog in de ontwerpfase en wordt geoutsourcet bij een extern bedrijf;
- Het gebruik van gezichtsherkenning aan de toegangspoort van bijvoorbeeld een kazerne. Dit project wordt samen ontwikkeld met CD&E, een autonome toegangspartij die extern is gesourced. Dit betreft een

project/experiment waarbij het de bedoeling is om als extra beveiligingslaag gezichtsherkenning te gebruiken. Dit gaat met name om grote evenementen, bijvoorbeeld als dit plaatsvindt op een kazerne. Als bijvoorbeeld geen herkenning plaatsvindt in een (vooraf aangelegde) database dan volgt extra fysieke screening (visitatie).

Verkorte aanbevelingen op ontwikkelingen

Betrek het Kenniscentrum Innovatie eXperimenten en Simulatie (hierna: KIXS) bij deze ontwikkelingen. Dit kenniscentrum van Defensie houdt zich bezig met innovatietrajecten bij Defensie. Mogelijk kunnen zij meedenken over dit traject en wat haalbaar is binnen de kaders van de wet- en regelgeving. Bovendien is er onlangs een Aanwijzing Kaders Data (Science) projecten vastgesteld door de Chief Information Officer (hierna: CIO) van Defensie.⁷⁶ Dit document bevat de nodige kaders op het gebied van privacy, fundamentele rechten en zeggenschap van burgers en militairen en ethische beginselen. Dit document kan helpen bij het opstellen van beleid en kaders waarvoor de AI en gezichtsherkenning aan moet voldoen.

Op het eerste gezicht lijkt het gelet op de huidige wet- en regelgeving niet toegestaan om bij de uitvoering van deze activiteit persoonsgegevens te verwerken. Hiervoor ontbreekt waarschijnlijk een grondslag. Bij de invulling van deze activiteiten en toetsing aan de Aanwijzing zal deze conclusie waarschijnlijk ook volgen.

⁷⁶ Chief Information Officer Defensie, 'Aanwijzing Kaders Data (Science) Projecten', vastgesteld 1 maart 2022.

Activiteit 5B

Omschrijving activiteit 5B

De AST's zijn zoekteams met specialisten en apparatuur van Defensie, bestaande uit militairen met kennis en ervaring, opgedaan tijdens missies en operaties in het buitenland - en Nederland zelf - over het onderkennen en doorzoeken van het gehele fysieke domein onder complexe omstandigheden. Ten behoeve van de algemene gereedstelling op inzet (bescherming eigen grondgebied en dat van bondgenoten, hoofdtak 1) en het ondersteunen bij rampenbestrijding (o.a. militaire bijstand of MSOB, hoofdtak 3) wordt onder meer gebruikgemaakt van realistische 'scenario's'. Daarvoor bestaat onder andere het Opleidings- en Trainingscentrum Genie. De noodzaak en het doel zijn gelegen in het zo realistisch mogelijk oefenen, vergelijkbaar met een daadwerkelijke inzet.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van de Genie, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

142

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht. Ook uit artikel 97 Gw kan geen wettelijke verplichting of taak van algemeen belang of openbaar gezag worden afgeleid.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub I van het AOD bepaalt dat het Ministerie van Defensie de Commandant Landstrijdkrachten als verantwoordelijke kent.

Artikel 13 AOD bepaalt het volgende:

“De Commandant Landstrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Landstrijdkrachten;*
- b. De gereedstelling en instandhouding van de landstrijdkrachten;*
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*

- d. *Het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Landstrijdkrachten;*
- e. *De advisering op het gebied van militair landoptreden."*

Subtaakbesluit Commando Landstrijdkrachten 2015

Artikel 26 AOD bepaalt dat de Commandant Landstrijdkrachten op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Het Subtaakbesluit Commando Landstrijdkrachten 2015 (hierna: subtaakbesluit) artikel 14, Het Opleidings- en Trainingscommando kent de volgende taken toe met betrekking tot training en opleiding:

"Het Opleidings- en Trainingscommando staat onder leiding van de Commandant Opleidings- en Trainingscommando die is belast met:

- a. *Het, met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Landstrijdkrachten, geven van de ambtelijke leiding aan het Opleidings- en Trainingscommando;*
- b. *Het operationeel gereed stellen van CBRN respons eenheid en het in stand houden van de gereedheidstatus;*
- c. *Het formeren, inzet gereed stellen en bijdragen aan de instandhouding van operationeel gereede respectievelijk ingezette CBRN respons eenheid;*
- d. *Het uitvoeren van nazorg en recuperatie van operationeel ingezette CBRN respons eenheid;*
- e. *Het ontwikkelen en verzorgen van in-, door- en uitstroomopleidingen;*
- f. *Het bieden van trainingsondersteuning op niveau 2 t/m 6;*
- g. *Het ontwikkelen en onderhouden van kennisproducten/doctrines op het gebied van landoptreden;*
- h. *Het coördineren van externe dienstverlening op gebied van opleiding en training en het toezien op conforme uitvoering;*
- i. *Het uitvoeren van militaire bijstand en militaire steunverlening;*
- j. *Het leveren van een bijdrage aan de informatiebehoefte van de Commandant Landstrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid."*

143

De activiteiten van AST's zijn voor zover het is gericht op het formeren en gereedstellen (opleiding en training) terug te voeren op het subtaakbesluit, in het bijzonder artikel 14 sub c.

Toepassingsbereik AVG

Materieel toepassingsbereik

Om militairen voor te bereiden op nationale inzet (militaire bijstand of MSOB) en/of inzet in het buitenland wordt gebruikgemaakt van 'scenario's'. De noodzaak en het doel zijn gelegen in het zo realistisch mogelijk oefenen, vergelijkbaar met een daadwerkelijke inzet. Om te trainen wordt gebruikgemaakt van oefenterreinen. Er zijn twee type oefenterreinen te onderscheiden:

- Militair oefenterrein. Voor AST trainingsactiviteiten zal trainen op een militair oefenterrein doorgaans plaatsvinden bij het Opleidings- en Trainingscentrum Genie. Naast dit afgebakende terrein zijn er ook meer vrijelijk begaanbare militaire oefenterreinen in Nederland. De respondent vraagt zich af binnen welke kaders het eventueel mogelijk is om persoonsgegevens van een voorbijganger te verwerken.⁷⁷ Bijvoorbeeld foto's van een auto (kenteken). De informatie wordt alleen gebruikt ten behoeve van de oefening en uitwerking daarvan.
- Willekeurige plek in Nederland. Defensie kan een strook (civiel gebied in Nederland) aanvragen en gebruiken om te oefenen met bijvoorbeeld een *unmanned aerial vehicle* (onbemand vliegtuig) (hierna: UAV). Een UAV kan met Laser Imaging Detection And Ranging (hierna: LiDAR) een multi-spectrale camera of een RGB camera zijn uitgerust. Op die foto's is het (hoewel beperkt) mogelijk om mensen te identificeren. Volgens de respondent is het blurren van mensen onwenselijk omwille van het creëren van een zo realistisch mogelijk scenario.

144

Om te kunnen trainen en opleiden ten behoeve van de algemene gereedstelling worden persoonsgegevens verwerkt. Er zijn verschillende situaties te onderscheiden waarbij het de vraag is of er een grondslag is om algemene en/of bijzondere persoonsgegevens te verwerken ten behoeve van de algemene gereedstelling. Het gaat om de volgende situaties:

- Verwerken van (gewone of bijzondere) persoonsgegevens van eigen Defensiepersoneel;
- Verwerken van (gewone of bijzondere) persoonsgegevens van ingehuurd externen (bijvoorbeeld acteurs);
- Verwerken van (gewone of bijzondere) persoonsgegevens van (toevallige) omstanders en burgers die zich bijvoorbeeld in een natuurgebied c.q. voor medegebruik beschikbaar oefenterrein bevinden of een willekeurig aangevraagd oefengebied op civiel terrein.

⁷⁷ Denk hierbij aan omstanders ingevolge "Recreatief medegebruik van defensie-terreinen"
https://puc.overheid.nl/mp-bundels/doc/PUC_432000001000_10/1/.

Aangezien vaststaat dat persoonsgegevens worden verwerkt valt het op grond van artikel 2 AVG binnen het materieel toepassingsbereik van de AVG.

Territoriaal toepassingsbereik

De verwerkingen vallen onder deze activiteit richten zich op Nederlanders en vinden plaats in Nederland. Dit doet zich voor onder de verantwoordelijkheid van de Minister van Defensie, voor zover het gaat om het verwerken van persoonsgegevens ten behoeve van de algemene gereedstelling.

De verwerkingen vallen binnen het territoriaal toepassingsbereik van de AVG. De AVG is dus van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen voor het verwerken van persoonsgegevens uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. In deze paragraaf lichten wij de relevante grondslagen toe.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens mogen worden verwerkt als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd waarbij het voor de betrokkene duidelijk moet zijn dat er persoonsgegevens worden verwerkt. Bovendien is het alleen toegestaan om persoonsgegevens op basis van deze grondslag te verwerken als het noodzakelijk is voor de vervulling van de publieke taak.

Activiteiten met betrekking tot de gereedstelling en instandhouding, waaronder opleiding en training vallen zijn als taak toebedeeld in artikel 13 sub b AOD en gespecificeerd in artikel 14 sub c subtaakbesluit. Om te kunnen trainen is het waarschijnlijk wel voorzienbaar dat enkele gewone persoonsgegevens van Defensiepersoneel en ingehuurde acteurs worden verwerkt. Denk hierbij aan het verwerken van de naam van een militair of acteur, maar ook persoonsgegevens die samenhangen met het maken van foto's of video's tijdens een oefening. Dat is lastiger voor wat betreft bijzondere persoonsgegevens zoals biometrische gegevens van militairen, omstanders of ingehuurde acteurs voor, tijdens of ten behoeve van een oefening. Het is immers op basis van het subtaakbesluit niet voorzienbaar dat hiervoor dit soort persoonsgegevens worden verwerkt.

Daarnaast is het niet *noodzakelijk* om persoonsgegevens te verwerken om deze taak uit te voeren.

De taak die voortvloeit uit het subtaakbesluit is volgens ons echter onvoldoende specifiek om aan te merken als een publieke taak voor het algemeen belang waarmee het mogelijk is om zelfstandig persoonsgegevens te verwerken. Aangezien het om zeer een algemene taak gaat, kan hier geen *bevoegdheid* om persoonsgegevens te verwerken aan worden ontleend. Het is daarom niet toegestaan om op grond van het algemeen belang persoonsgegevens van burgers of ingehuurd personeel te verwerken die zich op een oefenterrein begeven.

Daarnaast is het subtaakbesluit een ministeriële regeling, waardoor het – zelfs als op basis van de taakomschrijving voldoende voorzienbaar is dat er persoonsgegevens worden verwerkt – geen bevoegdheid kan scheppen in de zin van artikel 6 lid 1 sub e AVG. Om een dussdanige bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een subtaakbesluit mist deze rechtskracht. Concluderend heeft de krijgsmacht voor gereedstelling ten behoeve van (algemene voorbereiding) op inzet, waar training en opleiding onder vallen, geen zelfstandige bevoegdheden.⁷⁸

146

De grondslag om persoonsgegevens te verwerken ten behoeve van training en opleiding kan mogelijk voortvloeien uit toestemming uit hoofde van de uitvoering van de functie (uitvoering van de overeenkomst) of gerechtvaardigd belang. Deze grondslagen worden nader aangestipt.

Toestemming voor het verwerken van gewone persoonsgegevens

Voor gereedstelling en daarmee trainen en opleiden bestaan waarschijnlijk gelet op de bovenstaande uitwerking geen bevoegdheden om persoonsgegevens te verwerken op grond van het algemeen belang. Mogelijk kan in het kader van opleiding en training toestemming van de betrokkene worden gevraagd in de zin van artikel 6 lid 1 sub a AVG voor het verwerken van gewone persoonsgegevens. Op grond van artikel 4 onderdeel 11 AVG gaat het bij toestemming om een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting waarmee iemand met een verklaring of ondubbelzinnige actieve handeling een verwerking van persoonsgegevens aanvaardt. Het is dus niet toegestaan om enkel te informeren dat er een verwerking van persoonsgegevens zal plaatsvinden. Daarnaast is het niet toegestaan om druk

⁷⁸ DJZ april 2021, Algemene juridische kaders voor activiteiten in de informatieomgeving, p. 4.

uit te oefenen of negatieve consequenties te verbinden aan het weigeren tot het geven van toestemming.⁷⁹

Er zijn verschillende situaties waarin het vragen van toestemming van de betrokkene zich zou kunnen voordoen:

- Het vragen van toestemming voor het verwerken van algemene of bijzondere persoonsgegevens van eigen Defensiepersoneel;
- Het vragen van toestemming voor het verwerken van algemene of bijzondere persoonsgegevens van acteurs die meedoen aan een oefening;
- Het vragen van toestemming voor het verwerken van algemene of bijzondere persoonsgegevens van omstanders die zich bijvoorbeeld op een defensie terrein dat is opengesteld voor medegebruik ten behoeve van recreatie bevinden.

Het vragen van toestemming is voor trainen en opleiden echter alleen mogelijk in een *gecontroleerde setting*. De *deelnemers* moeten dan bekend zijn met het karakter van de oefening. Deelnemers van een oefening beperkt zich daarbij slechts tot eigen Defensiepersoneel en acteurs die meedoen aan een training. Het verwerken van persoonsgegevens van omstanders zonder hun wetenschap is niet toegestaan. Voor omstanders die zich op een voor medegebruik van recreanten opengesteld defensie terrein begeven wordt het waarschijnlijk lastig (lees: onwerkbaar) om rechtsgeldige toestemming te vragen. Dit geldt voor het verwerken van zowel de gewone als bijzondere persoonsgegevens. Omdat er een actieve handeling is vereist voor toestemming volstaat bijvoorbeeld een enkel informatieve opmerking op een informatiebord (bijvoorbeeld bij de toegang van een voor medegebruik van recreanten opengesteld defensie terrein) niet. Bovendien mag er in het kader van toestemming geen sprake zijn een duidelijke onbalans in de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke. Dit is bijvoorbeeld het geval in de verhouding overheid-burger en werkgever-werknemer. Dat betekent dat het vragen van toestemming van eigen Defensiepersoneel waarschijnlijk geen verwerkingsgrondslag kan zijn.⁸⁰

Toestemming voor het verwerken van bijzondere persoonsgegevens

Voor het verwerken van bijzondere persoonsgegevens op basis van de grondslag toestemming gelden bovendien nog strengere eisen. Omdat de wens is uitgesproken om te oefenen met biometrische gegevens bespreken we deze

⁷⁹ Autoriteit Persoonsgegevens, 30 april 2020, 'Boete voor het verwerken vingerafdrukken werknemers', Boetebesluit, https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/boetebesluit_vingerafdrukken_personeel.pdf.

⁸⁰ DJZ april 2021, Algemene juridische kaders voor activiteiten in de informatieomgeving, p.6.

categorie apart. Biometrische gegevens zijn ingevolge artikel 9 AVG te kwalificeren als bijzondere persoonsgegevens. Bijzondere persoonsgegevens zijn in de AVG extra beschermd. Het is ingevolge artikel 9 lid 2 AVG alleen mogelijk om biometrische gegevens (vingerafdrukken, gezichtsherkenning) te verwerken van militairen, ingehuurd acteurs of omstanders als hiervoor uitdrukkelijke toestemming wordt gevraagd. Het verkrijgen van uitdrukkelijke toestemming is met zwaardere waarborgen omkleed dan de ondubbelzinnige toestemming die is vereist voor het verwerken van gewone persoonsgegevens op basis van toestemming (art. 6 lid 1 sub a AVG).⁸¹

Uitvoering overeenkomst

Op grond van artikel 6 lid 1 sub b AVG is een verwerking rechtmatig als deze noodzakelijk is om een overeenkomst uit te voeren waarbij de betrokkene partij is. In dat kader is het verwerken van gewone persoonsgegevens van deelnemers tijdens een training of oefening rechtmatig. Daarbij gaat het bijvoorbeeld om namenlijsten van personen die aanwezig zijn bij een training of oefening. Ook foto's en video's die uitsluitend worden verwerkt voor trainingsdoeleinden kunnen onder deze grondslag vallen. Daarbij is het dus wel van belang dat de persoonsgegevens die worden verwerkt in lijn zijn met de aanstelling van de Defensiemedewerker. Zo kan bij de aanstelling van een genist worden verwacht dat er persoonsgegevens worden verwerkt in het kader van een training. In deze zin leggen wij de aanstelling uit als equivalent van een arbeidsovereenkomst.

148

Het is ook mogelijk dat er beeldmateriaal van voorbijgangers wordt gemaakt. Op deze mensen is de grondslag uitvoering van een overeenkomst uiteraard niet van toepassing. Er is geen grondslag om van deze mensen persoonsgegevens te verwerken. Naast voorbijgangers worden ook acteurs ingezet voor trainingen. Met deze acteurs sluit Defensie een overeenkomst. In dat kader is de grondslag uitvoering van een overeenkomst mogelijk wél van toepassing.

Tijdens het trainen is het niet toegestaan om bijzondere persoonsgegevens te verwerken. Op grond van artikel 9 lid 1 AVG is het namelijk niet toegestaan om bijzondere persoonsgegevens te verwerken, tenzij sprake is van een van de uitzonderingen van artikel 9 lid 2 AVG. Van deze uitzondering is in het onderhavige geval geen sprake.

⁸¹ Zie onder meer

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/wp259_rev_0.1_nl.pdf, p. 20.

Gerechtvaardigd belang

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak. In het geval dat het om een typisch bedrijfsmatige handeling van een overheidsinstantie gaat is dit onder niet duidelijk gedefinieerde kaders misschien een mogelijkheid. Naast dat er sprake moet zijn van een typisch bedrijfsmatige handeling van een overheidsinstantie moet het verwerken van persoonsgegevens noodzakelijk en evenredig zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. Een voorbeeld van een typisch bedrijfsmatige handeling van een overheidsinstantie is het beveiligen van overheidsgebouwen door middel van cameratoezicht. Een dergelijke bedrijfsmatige handeling wijkt namelijk niet af van private organisaties die het gerechtvaardigd belang hebben hun eigendommen (waaronder panden) te beveiligen.

Het is moeilijk om te beoordelen of het trainen van militair personeel als iets typisch bedrijfsmatig van een overheidsinstantie valt te bestempelen en daarmee als gerechtvaardigd belang te kwalificeren. Het verwerken van gewone persoonsgegevens, zoals de naam van een militair of acteur tijdens een training of is mogelijk wel een typisch bedrijfsmatige handeling die noodzakelijk is om te kunnen trainen met (eigen) Defensiepersoneel. Dit geldt overigens waarschijnlijk niet voor het verwerken van bijzondere persoonsgegevens van omstanders of ingehuurde acteurs. Om vast te stellen of er sprake is van een gerechtvaardigd belang is het noodzakelijk om een belangenafweging te maken. Het is aan de verwerkingsverantwoordelijke om de afweging te maken of het verwerken van persoonsgegevens noodzakelijk en evenredig is en dat het gerechtvaardigd belang van Defensie prevaleert boven het belang van de betrokkene. Voordat Defensie de grondslag van het gerechtvaardigd belang mag toepassen, moet zij daarvoor eerst nagaan of bij deze activiteit sprake is van een typisch bedrijfsmatige handeling van een overheidsinstantie.

Mogelijk knelpunt		Aanbeveling
<i>Juridisch (grondslag)</i>		
1.	Ondanks het bestaan van een Opleidings- en Trainingscentrum Genie waar het mogelijk is om realistische scenario's na te bootsen zonder het gebruik van persoonsgegevens. Echter kunnen er tijdens oefeningen mogelijk persoonsgegevens worden verwerkt. In het	<i>Formeel wettelijke grondslag</i> Het is aan de wetgever om wetgeving te creëren voor overheidsorganisaties waaruit taken en bevoegdheden zijn te ontleen. Deze taken en bevoegdheden moeten daarbij voldoende duidelijk en concreet zijn om te kwalificeren als grondslag in de zin van artikel 6 lid 1 sub e AVG. Het is

<p>verlengde daarvan zijn er vragen gesteld in welke gevallen dat is toegestaan en binnen welke kaders. Het wordt als gemis ervaren dat een grondslag ontbreekt om persoonsgegevens te verwerken ten behoeve van de algemene gereedstelling. Het gaat dan om het verwerken van persoonsgegevens in het kader van informatie gestuurd optreden (hierna: IGO).</p>	<p>daarom aan de wetgever om te bepalen of het wenselijk is dat AST's deze en/of soortgelijke activiteiten uitvoert. Wij adviseren in ieder geval om de taken en bijbehorende bevoegdheden op een heldere en voor de betrokkene duidelijke wijze vast te leggen in (formele) wetgeving waarbij de beginselen van de AVG in acht worden genomen.</p> <p><i>Verricht nader onderzoek naar de reikwijdte van typisch bedrijfsmatige handelingen</i></p> <p>Het is de vraag of de gewenste verzameling van persoonsgegevens ten behoeve van training en opleiding is aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie. Als dit namelijk het geval is dan zou een beroep op het gerechtvaardigd belang (artikel 6 lid 1 sub f AVG) mogelijk zijn, mits de verwerking gerechtvaardigd en noodzakelijk is en er een belangenafweging is uitgevoerd en aan de overige eisen van de AVG (in het bijzonder artikel 5 AVG) wordt voldaan. Het belang van Defensie moet hierbij wel prevaleren boven het belang van de betrokkene. Omdat in de wet- en regelgeving, rechtspraak en literatuur geen duidelijke definitie is gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie, is het lastig om te beoordelen of bij deze activiteit een beroep mogelijk is op het gerechtvaardigd belang.</p> <p><i>Virtuele oefenomgeving</i></p> <p>Het lijkt (technisch en praktisch) vrijwel onmogelijk om een realistisch virtueel</p>
--	--

		<p>oefenscenario te creëren. Door deze gepercipieerde onmogelijkheid zijn AST's mogelijk niet in staat om te trainen voor zover het gaat om oefenen waarbij informatie die te herleiden is naar een persoon – bijvoorbeeld biometrische gegevens – in voorkomt.</p> <p>Ontwikkelingen in de techniek volgen elkaar desalniettemin wél snel op. Het is zinvol om nader onderzoek te doen naar mogelijkheden en resultaten van het oefenen met gecreëerde oefenscenario's⁸² en fictieve datasets.</p>
--	--	--

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

151

Op dit moment is het onduidelijk of het voor een omstander voldoende duidelijk is dat er mogelijk persoonsgegevens verwerkt worden. Op de informatieborden staat hierover waarschijnlijk niets aangegeven. Informeren via een informatiebord kan mogelijk een onderdeel zijn om tot een rechtmatige toestemming te komen, maar schiet tekort op het vereiste van een actieve handeling. Een voorafgaande actieve ondubbelzinnige handeling is namelijk vereist om als betrokkene toestemming te verlenen.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel moet worden verwerkt. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

⁸² Zie ook Reactie op verzoek commissie over oefenmogelijkheden voor informatiegestuurd optreden, Tweede Kamer, vergaderjaar 2021–2022, 32 761, nr. 203, p. 3-4.

Er is geen indicatie dat er op dit moment tijdens een oefening persoonsgegevens worden verzameld om die vervolgens voor een ander, onverenigbaar doel verder te verwerken.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Bij deze activiteit is geen indicatie dat er meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

De persoonsgegevens die voor, na of tijdens een oefening worden verzameld kunnen zeer uiteenlopend zijn. Een groot deel van de persoonsgegevens, bijvoorbeeld het kenteken van een auto en foto's van burgers in een oefengebied zijn aan te merken als bijvangst. Defensie is hier niet specifiek naar op zoek. Uiteraard kan het gebeuren dat deze persoonsgegevens niet juist zijn. Er is een proces ingericht voor betrokkenen om inzage te verlenen en (op verzoek of indien nodig) te rectificeren.⁸³

152

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalst, dan moeten de persoonsgegevens worden gewist.

De respondent heeft expliciet aangegeven dat persoonsgegevens die voor een oefening worden verwerkt op een veilige laptop voor een vastgestelde periode worden bewaard en tijdig verwijderd.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen

⁸³ Privacyrechten persoonsgegevens, Ministerie van Defensie, <https://www.defensie.nl/onderwerpen/privacyrechten/privacyrechten-persoonsgegevens>.

ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De Genie neemt het Defensie Beveiligingsbeleid (hierna: DBB) bij deze activiteit in acht. Daarom is er een goed beveiligingsniveau voor de persoonsgegevens die worden verwerkt. De persoonsgegevens worden op die manier beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daarmee wordt aan het beginsel van integriteit en vertrouwelijkheid voldaan.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Er is geen inzicht gegeven in of de activiteit is opgenomen in het verwerkingsregister.

Conclusie

Het wordt noodzakelijk geacht (of in ieder geval wenselijk) om persoonsgegevens te verwerken ten behoeve van de algemene gereedstelling tijdens het trainen en opleiden om dit zo realistisch mogelijk te maken. Er is echter waarschijnlijk alleen een grondslag om gewone persoonsgegevens van eigen Defensiepersoneel te verwerken tijdens training en opleiding. Er lijkt geen grondslag te bestaan om gewone, bijzondere en/of gevoelige persoonsgegevens te verwerken van omstanders of burgers ten behoeve van een oefening in het kader van algemene gereedstelling. Onze aanbevelingen strekken tot het onderzoeken van de mogelijkheid van een formeel wettelijke grondslag, het verrichten van nader onderzoek naar typisch bedrijfsmatige handelingen voor een overheidsinstantie of tot het gebruik van een virtuele oefenomgeving en fictieve datasets.

Er ontbreekt mogelijk een sluitende grondslag om persoonsgegevens te verzamelen, terwijl dit in het kader van de algemene gereedstelling wel plaatsvindt. Daarom krijgt deze activiteit de kleur oranje.

Activiteit 6

Omschrijving activiteit 6

De oorspronkelijke activiteiten van Land Information Manoeuvre Centre (hierna: LIMC) liggen sinds november 2020 stil. Deze activiteiten zagen toe op het doen van onderzoek naar maatschappelijke ontwikkelingen en het in kaart brengen van desinformatie gedurende de coronapandemie. LIMC volgde hiervoor een Concept Development & Experimentation (hierna: CD&E) traject. Dat hield in dat aan de hand van nieuwe data-technologieën een overzicht van de (corona) toestand (Situational Awareness en Situational Understanding) werd gegenereerd. Aanleiding voor het stilzetten van de activiteiten was dat LIMC persoonsgegevens als 'bijvangst' verwerkte bij het verzamelen van deze informatie. Hiervoor was geen verwerkingsgrondslag. Op dit moment ontplooit LIMC geen activiteiten. Daarom verwerkt LIMC op dit moment geen persoonsgegevens.

De knelpunten die toezien op de rechtmatigheid - zoals opgenomen in het LIMC-rapport – zijn onder de huidige stand van zaken niet van toepassing.⁸⁴ LIMC wil in de toekomst wél activiteiten ontplooiën. Ten tijde van het schrijven van dit rapport is er geen zicht of en wanneer er weer activiteiten ontplooit mogen worden. De werkzaamheden die LIMC voor ogen heeft zijn als volgt:

154

LIMC wil aan de hand van onder meer Artificial Intelligence (hierna: AI) en data science toekomstig handelingsperspectief ontwikkelen. Dit in het kader van Informatie Gestuurd Optreden (hierna: IGO). Daarbij kijkt LIMC naar fenomenen en volgt dus geen personen. Die taak ligt namelijk bij de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). Het verzamelen van informatie richt zich daarbij op het gehele omgevingsbeeld, waarbij het alleen gaat om inzicht vergaren in trends, ontwikkelingen en fenomenen. De informatie die LIMC verzamelt is afhankelijk van de onderzoeksvraag. De gewenste activiteiten zien voornamelijk toe op hoofdtak 1 en 2 van Defensie.

Deze potentiële activiteit kan in drie verschillende fasen plaatsvinden:

1. Trainen. Het in kaart brengen én begrijpen van de dynamiek van het volledige operatiegebied - en de daarbij behorende sociale (virtuele) infrastructuur en bevolking - wordt in deze sterk gedigitaliseerde wereld steeds belangrijker. Goed voorbereide analisten zijn hiervoor essentieel. Succesvol zijn kan alleen als personeel voldoende kennis heeft van de omgeving waarin de operatie plaatsvindt. Volgens LIMC is het alleen mogelijk om dit tijdens inzet direct toe te passen als er wordt getraind met relevante (beschikbare) informatie. Relevante informatie verkrijgt

⁸⁴ Onderzoek naleving Algemene verordening gegevensbescherming – Experimenteeromgeving Land Information Manoeuvre Centre (LIMC), 31-03-2021.

LIMC onder andere uit openbare bronnen, waaronder sociale media. Aan de hand van een analyse van deze informatie kan LIMC zich voorbereiden op een situatie die zo dicht mogelijk bij de werkelijkheid komt. Het doel is hierbij uitdrukkelijk niet het verzamelen van persoonsgegevens. De respondenten merken daarbij op dat het onmogelijk is om goed te trainen en voor te bereiden zonder persoonsgegevens als 'bijvangst' te verwerken.

2. (Algemene) gereedstelling. In gevallen waar Defensie moet anticiperen op mogelijke inzet wil de krijgsmacht zich zo goed als mogelijk voorbereiden op de eventuele inzet. Daarvoor is het van belang om te weten wat de eventuele strategie en mogelijkheden van de (potentiële) tegenstander(s) zijn. Ook wil de krijgsmacht weten hoe de sociale, virtuele en fysieke infrastructuur van een land is en hoe deze met elkaar samenhangen. Deze informatie verzamelt LIMC door beschikbare (online) informatie te verzamelen en vervolgens te analyseren. Deze informatie zorgt er bijvoorbeeld voor dat de landmacht weet hoe het haar troepen het beste kan inzetten. Bovendien kan het duidelijk maken hoe het conflict zich verder ontwikkelt en hoe actoren hierop reageren. Het verwerken van persoonsgegevens, al dan niet als 'bijvangst', is hierbij onvermijdelijk.
3. Inzet. Op het moment dat er daadwerkelijk sprake is van inzet wil LIMC informatie over de vijand en de lokale bevolking in kaart brengen, analyseren en trends duiden, om daar tijdig op te reageren. LIMC zoekt dan bijvoorbeeld naar het sentiment dat leeft onder de lokale bevolking en of dit verschilt van alle betrokken actoren in het gebied. Door deze informatie te analyseren is het mogelijk om te anticiperen op een passende strategie en staat de krijgsmacht niet voor verrassingen.

155

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van LIMC, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub I van het AOD bepaalt dat het Ministerie van Defensie de Commandant Landstrijdkrachten als verantwoordelijke kent.

Artikel 13 AOD bepaalt over de Commandant Landstrijdkrachten het volgende:

“De Commandant Landstrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Landstrijdkrachten;*
- b. De gereedstelling en instandhouding van de landstrijdkrachten;*
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. Het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstcentra op te leveren producten en diensten ter ondersteuning van het Commando Landstrijdkrachten;*
- e. De advisering op het gebied van militair landoptreden.”*

Artikel 26 AOD bepaalt dat de Commandant Landstrijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft. Er is geen subtaakbesluit dat regelt dat LIMC bestaat als Defensieonderdeel of waar taken voor LIMC zijn opgenomen. Op basis hiervan kan deze activiteit niet worden aangemerkt als taak van LIMC.

156

Toepassingsbereik AVG

Materieel toepassingsbereik

Momenteel verwerkt LIMC geen persoonsgegevens omdat de activiteit is stilgelegd sinds november 2020. Bij de activiteit die ze voor ogen hebben worden – al dan niet als ‘bijvangst’ - wel persoonsgegevens verwerkt. Een voorbeeld hiervan is het verwerken van persoonsgegevens ten behoeve van de bronverwijzing. Een verwerking vindt dan al plaats door het vermelden van de auteur van de bron, bijvoorbeeld van een nieuwsartikel. De verwerking van persoonsgegevens in de activiteit die LIMC voor ogen heeft valt dus binnen het materieel toepassingsbereik van de AVG. Dit geldt tijdens het trainen, de algemene gereedstelling en de daadwerkelijke inzet.

Territoriaal toepassingsbereik

Bij de potentiële activiteit is de verwerkingsverantwoordelijke – de Minister van Defensie – gevestigd in Nederland. Daarom valt de verwerking van persoonsgegevens bij de potentiële activiteit op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

Kortom, op dit moment is de AVG niet van toepassing omdat LIMC geen activiteiten uitvoert. Op de activiteiten die LIMC voor ogen heeft is de AVG wel van toepassing.

Beoordeling activiteit

Bij deze activiteit werken we de beginselen van artikel 5 AVG niet allemaal uit. Dit komt omdat de beginselen uitvoerig zijn onderzocht en uitgewerkt in het LIMC-rapport en omdat er momenteel geen activiteiten plaatsvinden.⁸⁵ Om te bevestigen dat er geen grondslag is om persoonsgegevens te verwerken tijdens het trainen en de algemene gereedstelling werken we de rechtmatigheid wél verder uit. Daarbij gaan we in op de relevante verwerkingsgrondslagen van artikel 6 AVG.

Algemeen belang

Op grond van het AOD zijn er geen taken geformuleerd voor LIMC. Ook is er geen subtaakbesluit waar eventuele taken voor LIMC in zijn vastgelegd. Om die reden is er ook geen bevoegdheid om persoonsgegevens te verwerken ter uitvoering van een publieke taak voor het algemeen belang. Ook op het moment dat een taakomschrijving in een subtaakbesluit is opgenomen (waaruit voldoende voorzienbaar is dat daarbij persoonsgegevens worden verwerkt), levert dit geen bevoegdheid op om persoonsgegevens te verwerken in de zin van artikel 6 lid 1 sub e AVG. In dit geval kan LIMC geen beroep doen op de verwerkingsgrondslag algemeen belang. Om een bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een subtaakbesluit mist deze rechtskracht.

157

Gerechtvaardigd belang

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak. In het geval het om bedrijfsvoering gaat is dit wel een mogelijkheid. Daarbij moet het verwerken van persoonsgegevens noodzakelijk zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. De potentiële activiteit is niet te kwalificeren als bedrijfsvoering, omdat het niet is aan te merken als een typisch bedrijfsmatige handeling. Activiteiten die toezien op of samenhangen met gereedstellen/inzet van de krijgsmacht zijn in geen enkele zin aan te merken als een typisch bedrijfsmatige handeling. Daarom kan LIMC geen beroep doen op het gerechtvaardigd belang.

⁸⁵ Onderzoek naleving Algemene verordening gegevensbescherming – Experimenteeromgeving Land Information Manoeuvre Centre (LIMC), 31-03-2021. Dit rapport zag toe op de coronapandemie, maar is wel relevant omdat is onderzocht hoe LIMC omgaat met de beginselen van artikel 5 AVG.

Alleen als LIMC een verzoek vanuit het civiel gezag krijgt is het toegestaan om persoonsgegevens te verwerken, voor zover bij het civiele gezag wel een grondslag aanwezig is. LIMC heeft nog nooit een verzoek om bijstand ontvangen. Er is dus geen grondslag om zelfstandig – of op grond van bijstand – persoonsgegevens te verwerken gedurende het trainen en tijdens de algemene gereedstelling.

Mogelijke knelpunten

LIMC voert momenteel de (gewenste) activiteit niet uit omdat er geen grondslag is voor het verwerken van persoonsgegevens. Daarnaast zijn er mogelijke knelpunten signaleerd.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	<p>LIMC heeft geen zelfstandige grondslag om persoonsgegevens te verwerken.</p> <p>LIMC ervaart verschillende knelpunten bij het trainen van personeel en gedurende de algemene gereedstelling:</p> <p>a. Het verwerken van persoonsgegevens - al dan niet als 'bijvangst' - is onvermijdelijk. Het doel is uitdrukkelijk niet om persoonsgegevens te verwerken. Denk hierbij aan bronvermeldingen waarin LIMC verwijst naar artikelen. Als in die artikelen een naam voorkomt dan is dit een verwerking van persoonsgegevens. LIMC onderbouwt een standpunt (melding) door middel van (volledige, dat wil zeggen minimaal auteur en vindplaats) bronvermelding. LIMC ziet</p>	<p>LIMC heeft nagedacht over het werken met zelf gecreëerde oefenscenario's.</p> <p>Volgens de respondenten is het vrijwel onmogelijk om een <u>realistisch</u> oefenscenario te creëren met denkbeeldige landen/partijen/actoren die de complexiteit van onderlinge verwevenheden tussen bijvoorbeeld de bevolking en strijdende actoren nabootsen. Hiervoor is een enorme hoeveelheid aan data nodig. Door deze onmogelijkheid is LIMC niet in staat om realistisch te trainen of voor te bereiden. Het creëren van een alomvattende fictieve situatie is met de huidige stand van de techniek niet mogelijk. Ontwikkelingen in de techniek volgen zich wél snel op. Het is zinvol om nader onderzoek te doen naar mogelijkheden en resultaten van het oefenen met gecreëerde oefenscenario's.</p> <p>Mocht dit geen oplossing bieden dan is het enkel mogelijk om persoonsgegevens te verwerken als er</p>

	<p>de waarschijnlijkheid dat een melding 'betrouwbaar' is met twee bronnen als 'waarschijnlijk' en met drie bronnen als 'bevestigd'. Een goede onderbouwing met bronnen zónder persoonsgegevens is in die zin lastig;</p> <p>b. Er ontstaat een enorme achterstand op de vijand als LIMC tijdens het trainen of tijdens de algemene gereedstelling geen informatie kan analyseren. Als je je analisten niet traint op wat ze moeten verwachten, dan kunnen ze tijdens de daadwerkelijk inzet geen verbanden leggen. Door deze kennisachterstand weet het Defensiepersoneel op voorhand niet goed wat te verwachten. Het duurt vaak enige tijd om tijdens inzet de situatie te begrijpen en signalen te duiden;</p> <p>c. Informatieachterstand bij een eventuele inzet heeft verschillende negatieve gevolgen. Allereerst kan het Defensiepersoneel de activiteiten niet goed aanvliegen, omdat onduidelijk is wat de</p>	<p>een formeel wettelijke grondslag wordt gecreëerd. Als daaruit voldoende duidelijk is dat er persoonsgegevens worden verwerkt, kan LIMC een beroep doen op de grondslag publieke taak (artikel 6 lid 1 sub e AVG).</p>
--	---	--

	<p>strategie en structuur van de vijand in het operatiegebied is. Ten tweede is het voor de krijgsmacht moeilijk om in te schatten welke troepen op welke locatie nodig zijn. Het gevolg daarvan is dat er onnodig slachtoffers vallen en opgedragen opdrachten onhaalbaar zijn. In dat stadium is het al 'te laat' om IGO in te zetten. Anticiperen op de toekomst aan de hand van IGO is dan een kennelijke onmogelijkheid.</p>	
<i>Organisatorisch</i>		
2.	<p>Defensieonderdelen kunnen een informatieverzoek indienen bij de MIVD. Het is niet bekend of de MIVD aan verzoeken voldoet die toezien op het aanleveren van de informatie die LIMC wil verzamelen. Ook is onbekend onder welke voorwaarden een informatieverzoek wel of niet wordt beantwoord.</p> <p>Mogelijk beschikt de MIVD over onvoldoende capaciteit (mankracht) om dit soort onderzoeken uit te voeren.</p>	<p>De MIVD opereert voor het uitvoeren van inlichtingenactiviteiten onder de Wet op de inlichtingen- en veiligheidsdiensten 2017(hierna: Wiv 2017). LIMC is geen inlichtingendienst en valt onder het Commando Landstrijdkrachten. Daarom valt LIMC niet onder de Wiv 2017 met bijbehorende kaders en systemen van toezicht.</p> <p>De MIVD is als onderdeel van Defensie verweven met de krijgsmacht. Als gezaghebbende inlichtingenpositie vergaren, verwerken en analyseren zij relevante en betrouwbare informatie om hiermee beslissend te kunnen handelen op strategisch niveau tot inzet van operationeel-tactische eenheden.</p> <p>Naast deze primaire taakstelling ondersteunt de MIVD ook de</p>

		<p>krijgsmachtonderdelen met inlichtingenopleidingen en innovaties. Bovendien heeft de MIVD een operationeel partnerschap met het Defensie Cyber Commando (hierna: DCC).⁸⁶</p> <p>Gelet op de mogelijke problematiek die LIMC ervaart met de onderlinge informatieachterstand is het raadzaam om de samenwerking tussen de Defensieonderdelen en de MIVD te evalueren.</p>
--	--	---

Conclusie

Momenteel is er bij deze activiteit geen grondslag om persoonsgegevens te verwerken tijdens het trainen en gedurende de algemene gereedstelling. Zolang er geen grondslag is om persoonsgegevens te verwerken, kunnen de gewenste activiteiten niet plaatsvinden. Andere activiteiten waarbij geen persoonsgegevens worden verwerkt door LIMC zijn in dit onderzoek niet meegenomen. Omdat er voor de gewenste activiteit geen grondslag is, krijgt deze activiteit de kleur rood.

⁸⁶ Jaarverslag MIVD 2020, p. 30-31.

Activiteit 7

Omschrijving activiteit 7

Het kan voorkomen dat mensen betogingen of demonstraties willen houden bij locaties/vliegvelden van de Commando Luchtstrijdkrachten (hierna: CLSK). In sommige gevallen plaatsen deze mensen op internet dat zij voornemens zijn om dit te doen. Bijvoorbeeld via sociale media. Naast berichten over betogingen kunnen er ook andere soorten berichten voorbij komen. Daarbij gaat het bijvoorbeeld om TESSOC-uitlatingen (Terrorism Espionage Subversion Sabotage Organised Crime). CLSK heeft enkel interesse in uitlatingen die toezien op eigendommen, medewerkers, gebouwen en vliegvelden van CLSK. Op dit moment is het voor security medewerkers lastig of zij actief opzoek mogen gaan naar dit soort dreigingen en uitlatingen. Ook is het voor security medewerkers lastig als medewerkers van CLSK een uitlating zijn tegengekomen (bijvoorbeeld op Facebook) en hiervan melding maken. Het is voor de security medewerkers onduidelijk welke gegevens ze mogen raadplegen en verwerken in verband met de Algemene verordening gegevensbescherming (hierna: AVG). Er is ook geen capaciteit ingericht die deze werkzaamheden verricht. Aangezien er bij het opzoeken van dit soort informatie persoonsgegevens als 'bijvangst' worden verwerkt, heeft CLSK deze activiteiten stilgelegd. CLSK wil wel simpele zoekacties verrichten om zo potentiële dreigingen voor te zijn. Op dit moment vindt deze activiteit niet plaats, daarom wordt gesproken over potentiële activiteit. Voor security medewerkers van vliegvelden voelt de situatie wrang, omdat ze op dit moment volgens hen te weinig informatie op kunnen zoeken. Daarnaast is onduidelijk of en hoe potentieel relevante informatie (bijvoorbeeld uitlatingen op Twitter waargenomen via een privéaccount) kan worden doorspeeld binnen de luchtmachtorganisatie.

162

Op het moment dat er grote evenementen zijn, zoals open dagen, is er wel een traject ingeregeld. Bij grote activiteiten worden namelijk de politie en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD) betrokken. Als er dan bepaalde dreigingen zijn dan brengt de MIVD of de politie, CLSK hiervan op de hoogte. Op die manier kan CLSK acteren op potentiële dreigingen. Op het moment dat er geen grote evenementen of dreigingen zijn, dan is er volgens CLSK een grijs gebied. In die gevallen krijgen ze namelijk geen informatie aangeleverd van de politie of de MIVD. In die gevallen ervaart CLSK het als onprettig om een passieve en afwachterende rol in te nemen. Zo kan het namelijk voorkomen dat ze voor verrassingen komen te staan. Als er dan alsnog demonstraties of TESSOC-activiteiten plaatsvinden levert dit in sommige gevallen materiële schade en/of reputatieschade op.

Een voorbeeld uit de praktijk waarin dit grijze gebied ook daadwerkelijk tot problemen heeft geleid ging als volgt. Een persoon wilde een foto maken in een

straaljager voor een tv-programma om de beveiliging van een vliegveld aan de kaak te stellen. Dit soort situaties wil CLSK mogelijk voorkomen door 'simpele' zoekacties te kunnen doen op het internet. Bijvoorbeeld zoeken op een vliegbasis en kijken of hier op internet (en sociale media) over wordt geschreven. Hierbij is CLSK niet geïnteresseerd in personen. Deze informatie willen ze verzamelen om de omvang van een dreiging te duiden. Ook kunnen ze de politie op de hoogte brengen van een eventuele dreiging.

De respondenten merken op dat er momenteel een spagaat is tussen enerzijds grote evenementen waar de politie en de MIVD voor dreigingen waarschuwt en anderzijds kleinere betogingen of TESSOC-activiteiten waarbij ze zelf niet op zoek kunnen gaan naar informatie. De politie en MIVD houden zich namelijk niet doorlopend bezig met zoekacties naar kleinere dreigingen van betogingen of TESSOC-activiteiten bij locaties van CLSK. Naar aanleiding van het Land Information Manoeuvre Centre (hierna: LIMC) heerst er volgens de respondenten een enorme terughoudendheid binnen Defensie. Bij zelfs de meest geringe twijfel of iets in lijn is met de AVG, wordt een activiteit niet uitgevoerd. Daarbij wordt te weinig onderzoek gedaan naar de mogelijkheden om een activiteit te ontplooiën binnen de kaders van de AVG.

CLSK betreft de AVG-coördinator vaak tijdig. De AVG-coördinator heeft geadviseerd om de potentiële activiteit niet uit te voeren, omdat er twijfel bestaat of het wel is toegestaan.

163

Alle vliegvelden (op één na) worden beveiligd door de Defensie Bewakings- en Beveiligingsorganisatie (hierna: DBBO). Zij lopen in de praktijk tegen dit probleem aan.

Binnen CLSK bestaat de wens om capaciteit beschikbaar te hebben die zich bezighoudt met kleine zoekacties. Daarbij is het doel uitdrukkelijk niet om persoonsgegevens te verwerken. Ze willen hierbij de mogelijkheid hebben om zoektermen te hanteren, zoals de vliegbasis in combinatie met bepaalde dreigingen. De frequentie is afhankelijk van het aantal dreigingen dat op dat moment voorkomt. Op dit moment zijn er relatief weinig demonstraties en dreigingen. CLSK wil voorbereid zijn op tijden waarin het aantal demonstraties toeneemt. Bij andere Europese landen zijn op dit moment bijvoorbeeld wel veel demonstraties. Als dat in Nederland ook toeneemt, wil CLSK weten hoe ze in lijn met de AVG kunnen handelen.

Momenteel is er geen document aanwezig waarin het juridisch kader voor CLSK wordt beschreven. De respondenten spreken de wens uit om een protocol/document te hebben waaruit zij alle informatie en kaders kunnen halen welke activiteiten wel/niet in lijn zijn met de AVG.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van CLSK en DBBO, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

CLSK

Grondwet

Artikel 44 Gw bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministeries staan onder leiding van een minister. Bij koninklijk besluit is het Ministerie van Defensie ingesteld.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub m van het AOD bepaalt dat het Ministerie van Defensie de Commandant Luchtstrijdkrachten als verantwoordelijke kent.

Artikel 14 AOD bepaalt over de Commandant Luchtstrijdkrachten het volgende:

"De Commandant Luchtstrijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Luchtstrijdkrachten;*
- b. de gereedstelling en instandhouding van de luchtstrijdkrachten;*
- c. het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Luchtstrijdkrachten;*
- e. de advisering op het gebied van militair luchtoptreden."*

164

Artikel 26 AOD bepaalt dat de Commandant Luchtstrijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Luchtstrijdkrachten 2018

Uit het subtaakbesluit volgt geen interne taaktoebedeling voor CLSK die toeziet op het bewaken en beveiligen van vliegvelden en andere objecten en personen van CLSK. Toch zijn er wel verschillende regelingen op basis waarvan

iedere militair belast kan zijn met bewakings- en beveiligingstaken.⁸⁷ Op dit moment wordt een groot gedeelte van de objecten van CLSK beveiligd door DBBO. Toch voert CLSK zelf ook beveiligingstaken uit, bijvoorbeeld bij vliegbasis Volkel. Omdat iedere militair belast kan zijn met bewakings- en beveiligingstaken kan dit ook worden aangemerkt als interne taak van militairen of burgerpersoneel van CLSK. DBBO beveiligt een groot deel van vliegbases en luchtmachtonderdelen, daarom bespreken we ook de interne taakstelling van DBBO.

DBBO

Grondwet

Artikel 44 Gw bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministeries staan onder leiding van een minister. Bij koninklijk besluit is het Ministerie van Defensie ingesteld.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub o AOD bepaalt dat het Ministerie van Defensie de Commandant Defensie Ondersteuningscommando als verantwoordelijke kent.

Artikel 16 AOD bepaalt over de Commandant Defensie Ondersteuningscommando het volgende:

165

“De Commandant Defensie Ondersteuningscommando is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van ambtelijke leiding aan het Defensie Ondersteuningscommando;*
- b. het binnen de kaders wereldwijd en zoveel mogelijk geïntegreerd leveren van producten en diensten op de terreinen huisvesting, beveiliging, facilitaire diensten, transport, catering, P&O dienstverlening, gezondheidszorg en opleidingen aan alle Defensieonderdelen en het waarborgen van de kwaliteit van de dienstverlening op die gebieden;*
- c. het verzorgen van rijksbreed categoriemanagement voor de aan Defensie toegewezen categorieën die bij het Defensie Ondersteuningscommando zijn belegd;*
- d. infrastructuurprojecten binnen de kaders van het defensiematerieelproces (DMP);*
- e. de advisering op de toegewezen functiegebieden en het van daaruit ondersteunen van de overige defensieonderdelen.”*

⁸⁷ Denk hierbij aan de Rijkswet geweldgebruik bewakers militaire objecten, Rijksbesluit inhoudende aanwijzing van te bewaken en te beveiligen objecten en Besluit geweldgebruik defensiepersoneel in de uitoefening van de bewakings- en beveiligingstaak.

Artikel 26 AOD bepaalt dat de Commandant Defensie Ondersteuningscommando op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leiding geeft.

Subtaakbesluit Commando Dienstencentra 2012⁸⁸

Het Commando DienstenCentra (hierna: CDC) is de voorloper van het huidige Defensie Ondersteuningscommando (hierna: DOSCO). Artikel 1 lid 1 sub e jo lid 4 sub c van het subtaakbesluit Commando Dienstencentra 2012 (hierna: subtaakbesluit) bepaalt dat het Commando Dienstencentra bestaat uit de Divisie Vastgoed & Beveiliging en dat DBBO daar weer onder valt.

Artikel 6 van het subtaakbesluit kent de volgende taken toe aan de Divisie Vastgoed & Beveiliging:

"De Divisie Vastgoed & Beveiliging staat onder leiding van de Commandant van de Divisie Vastgoed & Beveiliging die is belast met:

- a. het met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Commando Dienstencentra geven van ambtelijke leiding aan de Divisie Vastgoed & Beveiliging;*
- b. het leveren van diensten op het gebied van de nieuwbouw, het beheer, de instandhouding en afstoting van vastgoed ten behoeve van het Ministerie van Defensie, op basis van de door de Bestuursstaf gestelde kaders;*
- c. het leveren van diensten op het gebied van beveiligen en bewaken van defensieobjecten;*
- d. de verantwoordelijkheid voor de bedrijfsvoering van de Divisie Vastgoed & Beveiliging;*
- e. het fungeren als aanspreekpunt van de Divisie Vastgoed & Beveiliging voor klanten en opdrachtgevers;*
- f. het in overleg met de klant c.q. opdrachtgever doen vaststellen van de leveringsvoorwaarden van producten en diensten van de Divisie Vastgoed & Beveiliging binnen de randvoorwaarden van de Commandant Commando Dienstencentra en de Bestuursstaf;*
- g. de informatievoorziening ten behoeve van de Commandant."*

166

Op grond van artikel 6 sub c subtaakbesluit Commando Dienstencentra 2012 is het beveiligen en bewaken van defensieobjecten aan te merken als interne

⁸⁸ Het Commando Dienstencentra (hierna: CDC) is de voorloper van de huidige Defensie Ondersteuningscommando. Er is geen subtaakbesluit gevonden aangaande DOSCO. Vanwege deze omstandigheid is aansluiting gezocht en gevonden bij het subtaakbesluit CDC 2012 en de bijbehorende (zoveel mogelijk overeenkomende) terminologie.

taak voor DBBO. In het Rijksbesluit aanwijzing van te bewaken en te beveiligen objecten van 14 september 2000 zijn de te bewaken objecten aangewezen.⁸⁹ Uit de bijlage bij dit besluit volgt dat militaire vliegbases en vliegkampen, vluchtleidings- en gevechtsleidingscentra, alsmede militaire gedeelten van civiele luchtvaartterreinen zijn aangewezen als vaste defensieobjecten. Luchtvaartuigen zijn aangemerkt als mobiele objecten. Het bewaken en beveiligen van deze objecten is dus aan te merken als interne taak van DBBO.

Toepassingsbereik AVG

De AVG is van toepassing als de activiteit binnen het materieel en territoriaal toepassingsgebied van de AVG valt.

Materieel toepassingsbereik

Op het moment dat security medewerkers onderzoek gaan naar uitlatingen op het internet en sociale media is het doel daarvan uitdrukkelijk niet om persoonsgegevens te verwerken. Er worden wel persoonsgegevens als 'bijvangst' verwerkt. Ook daarop is de AVG van toepassing. Deze (potentiële) activiteit valt dus binnen het materieel toepassingsbereik van de AVG.

Territoriaal toepassingsbereik

Als de potentiële activiteit wordt uitgevoerd verwerkt DBBO persoonsgegevens onder verantwoordelijkheid van de Minister van Defensie. Deze persoonsgegevens worden tevens in Nederland verwerkt. Op basis daarvan valt de potentiële activiteit binnen het territoriaal toepassingsbereik van de AVG.

De AVG is dus van toepassing op deze potentiële activiteit.

Beoordeling activiteit

Aangezien de activiteit momenteel niet wordt ontplooid worden niet alle beginselen van artikel 5 AVG getoetst. Wel toetsen we de rechtmatigheid om te beoordelen of de activiteit eventueel uitgevoerd kan worden.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. In deze paragraaf worden de meest relevante grondslagen besproken.

Algemeen belang

⁸⁹ Staatscourant 2000/185 p. 16, alsmede het Wijzigingsbesluit houdende aanwijzing van te bewaken en te beveiligen objecten van 19 augustus 2008 (Staatscourant 2008, 159 pag. 6).

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens verwerkt mogen worden als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd waarbij het voor de betrokkene duidelijk moet zijn dat er persoonsgegevens worden verwerkt. Bovendien is het enkel toegestaan om persoonsgegevens op basis van deze grondslag te verwerken als het noodzakelijk is voor de vervulling van de publieke taak.

Wij zijn van mening dat artikel 6 sub c subtaakbesluit onvoldoende specifiek is omschreven, waardoor daaruit niet voorzienbaar is dat er persoonsgegevens kunnen worden verwerkt. Daarnaast is het subtaakbesluit een ministeriële regeling, waardoor het – zelfs als op basis van de taakomschrijving voldoende voorzienbaar is dat er persoonsgegevens worden verwerkt – geen bevoegdheid kan scheppen in de zin van artikel 6 lid 1 sub e AVG. Om een dusdanige bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een subtaakbesluit mist deze rechtskracht.

Gerechtvaardigd belang

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak. In het geval dat het om een typisch bedrijfsmatige handeling van een overheidsinstantie gaat is dit wel een mogelijkheid.⁹⁰ Daarbij moet het verwerken van persoonsgegevens noodzakelijk zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. Een beroep op het gerechtvaardigd belang is voor overheidsinstantie overigens niet mogelijk wanneer de verwerking plaatsvindt in het kader van de uitoefening van haar publieke taken.⁹¹

Een voorbeeld van een typisch bedrijfsmatige handeling van een overheidsinstantie is het beveiligen van gebouwen. Dit wijkt namelijk niet af van private organisaties. Bij deze activiteit gaat het om het beveiligen van vliegbases en luchtmachtonderdelen door het verrichten van zoekacties in het digitale domein. Toch is het de vraag of het verrichten van simpele zoekacties op het internet kan worden gezien als een typisch bedrijfsmatige handeling van een overheidsinstantie. Door de toenemende digitalisering en creatie van een informatiesamenleving kunnen we ons voorstellen dat de beveiligingstaak als mogelijk typisch bedrijfsmatige handeling van een overheidsinstantie zich mogelijk ook kan gaan uitstrekken over het digitale domein. De reikwijdte en afbakening daarvan zijn daarmee echter niet gegeven.

⁹⁰ Zie Memorie van toelichting op AVG, Kamerstukken II 2017/18, 2034 851, nr. 3, p. 37

⁹¹ Zie Tekst & Commentaar Algemene verordening gegevensbescherming, p. 92.

Als deze potentiële activiteit zich als een typisch bedrijfsmatige handeling van een overheidsinstantie kwalificeert dan zou een beroep op het gerechtvaardigd belang mogelijk zijn, mits de verwerking gerechtvaardigd en noodzakelijk is en er een belangenafweging is uitgevoerd. Waarbij het belang van Defensie moet prevaleren boven het belang van de betrokkene. Bovendien moet dan uiteraard ook aan de overige eisen van de AVG (in het bijzonder artikel 5 AVG) worden voldaan.

Het is lastig om te beoordelen wat een typisch bedrijfsmatige handeling van een overheidsinstantie precies inhoudt en hoe ver de beveiligingstaak precies reikt. In de wet- en regelgeving, de literatuur en de rechtspraak is namelijk geen duidelijke definitie gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie. De inzet van beveiligingscamera's wordt bijvoorbeeld over het algemeen (afhankelijk van de plaatsing) wel als typisch bedrijfsmatige handeling van een overheidsinstantie gezien. De digitale beveiliging waar deze activiteit op toeziet bevindt zich in een grijs gebied, omdat onduidelijk is of dit een typisch bedrijfsmatige handeling is. Deze problematiek speelt mogelijk bij meerdere overheidsinstanties. Naar deze problematiek is nader onderzoek vereist.

Toch vragen wij ons af of het op internet opsporen van betogingen of TESSOC-activiteiten valt aan te merken als een typisch bedrijfsmatige handeling van overheidsinstanties. Omdat het onder beveiliging valt kan hierover discussie bestaan. Voor nu kunnen we dus niet de conclusie trekken of er wel of geen sprake is van een gerechtvaardigd belang.

Onduidelijk is of CSLK en DBBO in dit kader een grondslag hebben om persoonsgegevens te verwerken. Er wordt dus mogelijk niet voldaan aan het beginsel van rechtmatigheid.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het is onduidelijk of er een grondslag is om persoonsgegevens te verwerken in het kader van het digitaal opzoeken van mogelijke dreigingen ter beveiliging van vliegbases en luchtmachtonderdelen.	<i>Verricht nader onderzoek naar de reikwijdte van typisch bedrijfsmatige handelingen</i> Het is de vraag of het verrichten van simpele zoekacties op het internet is aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie. Als dit namelijk het geval is dan zou een beroep op het gerechtvaardigd belang (artikel 6 lid

	<p>1 sub f AVG) mogelijk zijn, mits de verwerking gerechtvaardigd en noodzakelijk is en er een belangenafweging is uitgevoerd en aan de overige eisen van de AVG (in het bijzonder artikel 5 AVG) wordt voldaan. Het belang van Defensie moet hierbij wel prevaleren boven het belang van de betrokkene. Omdat in de wet- en regelgeving, rechtspraak en literatuur geen duidelijke definitie is gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie, is het lastig om te beoordelen of bij deze activiteit een beroep mogelijk is op het gerechtvaardigd belang.</p> <p><i>Creëer een formeel wettelijke grondslag</i></p> <p>Indien deze activiteit niet is aan te merken als typisch bedrijfsmatige handeling van een overheidsinstantie, maar wel mogelijk een publieke taak zou moeten worden van CLSK en DBBO dan moet hiervoor wetgeving worden gemaakt. Hoewel hierboven verschillende verwerkingsgrondslagen zijn aangestipt zijn de kaders van deze grondslagen mogelijk te beperkt om aan de behoefte van CLSK of DBBO te voldoen. Door middel van het creëren van een formeel wettelijke grondslag waaruit duidelijk is af te leiden welke persoonsgegevens worden verwerkt en welke noodzaak daarvoor is kan de grondslag van het algemeen belang (artikel 6 lid 1 sub e AVG) worden gebruikt. De verwerking van persoonsgegevens (ook als 'bijvangst') moet namelijk</p>
--	--

		voorzienbaar zijn bij een wet in de formele zin.
--	--	--

Mogelijke knelpunten

Naast het knelpunt dat toeziet op de rechtmatigheid, zijn tijdens het interview nog meer mogelijke knelpunten aan bod gekomen:

Mogelijke knelpunten		Aanbevelingen
<i>Organisatorisch</i>		
2.	Momenteel is er binnen CLSK 1,5 Fte aanwezig die zich bezighoudt met privacy. Volgens de respondenten is dit te weinig. Hierdoor zijn Data Protection Impact Assessments (hierna: DPIA's) nog niet uitgevoerd waar dit wel moet en worden er werknemers zonder privacykennis aangewezen om DPIA's uit te voeren. Voorbeelden hiervan zijn de sensoren op verschillende platformen (vliegtuigen/straaljagers). Op al deze sensoren is nog geen DPIA uitgevoerd. Ze worden momenteel wel ingezet.	Creëer capaciteit Richt de organisatie zo in dat er voldoende capaciteit is om privacyvraagstukken, waaronder DPIA's op te pakken. Zorg er ook voor dat er voldoende mensen zijn die kennis hebben van de AVG en overige verwante wet- en regelgeving die toezien op privacy.
<i>Ethisch</i>		
3.	Volgens de respondenten heerst er naar aanleiding van LIMC angst om activiteiten uit te voeren waarbij persoonsgegevens komen kijken. Als er momenteel twijfel bestaat of het verwerken van persoonsgegevens in lijn is met de AVG, vindt de activiteit geen doorgang. Volgens de respondenten wordt daarbij te weinig onderzoek gedaan hoe een activiteit alsnog in lijn met AVG ontplooid kan worden.	<i>Gerechtvaardigd belang</i> Door het mogelijk ontbreken van een grondslag om persoonsgegevens te verwerken zijn veel activiteiten waarbij persoonsgegevens worden verwerkt momenteel stilgezet. Door het ontbreken van een formeel wettelijke grondslag kan er geen beroep worden gedaan op het algemeen belang. Dat neemt niet weg dat typische bedrijfsmatige handelingen wel door kunnen gaan. In die gevallen kan de grondslag gerechtvaardigd belang namelijk van toepassing zijn, mits hierbij een belangenafweging wordt gemaakt

	<p>en de verwerking noodzakelijk is. Dit betekent dat er dus mogelijk wel activiteiten doorgang kunnen vinden die nu stil liggen. Dat geldt overigens niet voor deze potentiële activiteit.</p> <p><i>Vergroot bewustwording</i> Door het vergroten van de bewustwording en kennis van de AVG onder de medewerkers van CLSK wordt de LIMC-kramp deels weggenomen. Medewerkers weten hierdoor namelijk wat de (on)mogelijkheden zijn met betrekking tot de AVG.</p> <p>De respondenten hebben de wens uitgesproken om bijvoorbeeld protocollen op te stellen waardoor het voor medewerkers duidelijk wordt welke activiteiten wel/niet in lijn zijn met de AVG. Voor deze potentiële activiteit zien de respondenten het voor zich dat er een protocol komt waarin staat welke zoektermen gebruikt mogen worden en hoe het bijvoorbeeld zit met bewaartermijnen. Op die manier wordt de inbreuk voor de betrokkenen zo klein mogelijk. Het lastige is echter dan de AVG zo is ingericht dat zonder het hebben van een grondslag geen persoonsgegevens mogen worden verwerkt. Dit maakt het lastig om dergelijke protocollen op te stellen, zonder dat er een grondslag is in de zin van artikel 6 AVG. Voor deze activiteit is dit dus alleen mogelijk als er wordt geconcludeerd dat er sprake is van een gerechtvaardigd belang of als er een formeel wettelijke grondslag wordt gecreëerd.</p>
--	--

Conclusie

Momenteel is het onduidelijk of er een grondslag is om persoonsgegevens te verwerken bij deze potentiële activiteit. Het doel van de activiteit is uitdrukkelijk *niet* om persoonsgegevens te verwerken, maar bij de zoekslagen is het onvermijdelijk om geen persoonsgegevens te verwerken als bijvangst. Het is een grijs gebied of er in dit geval sprake is van een typisch bedrijfsmatige handeling van een overheidsinstantie waarbij een beroep op de grondslag van het gerechtvaardigd belang (conform artikel 6 lid 1 sub f) open staat. Nader onderzoek naar de reikwijdte van een typisch bedrijfsmatige handeling van overheidsinstanties is hierbij vereist, al bestaat deze onduidelijkheid waarschijnlijk bij meer overheidsinstanties. Deze onduidelijkheid is mede ingegeven door het ontbreken van rechtspraak, wet- en regelgeving en onderbouwende definities in de literatuur. Voor nu adviseren wij om in ieder geval nader onderzoek te verrichten naar dit grijze gebied en de reikwijdte van typisch bedrijfsmatige handelingen van overheidsinstanties voordat deze activiteit wordt uitgevoerd.

Indien deze activiteit niet is aan te merken als typisch bedrijfsmatige handeling van een overheidsinstantie maar wel mogelijk een publieke taak zou moeten worden van CLSK en DBBO, dan moet hiervoor wetgeving worden gemaakt. Indien er een formele wet zou zijn waarin taken en bevoegdheden zijn gecreëerd kan de activiteit namelijk op basis van deze grondslag (conform artikel 6 lid 1 sub e) mogelijk wel doorgang vinden.

173

Vanuit de respondenten is de wens uitgesproken dat er een kader/protocol wordt opgesteld waarin precies wordt aangegeven wat medewerkers van CLSK wel en niet kunnen doen in verband met de AVG. In het kader van deze activiteit is daarbij overwogen dat daarin wordt toegelicht welke zoekslagen wel uitgevoerd mogen worden en wat vervolgens met de persoonsgegevens gedaan moet worden. Bijvoorbeeld met de bewaartermijnen. Het lastige is echter dat de AVG zo is ingericht dat zonder het hebben van een grondslag geen persoonsgegevens mogen worden verwerkt. Als de conclusie is dat er een grondslag zou kunnen zijn (bijvoorbeeld omdat de activiteit valt aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie) dan adviseren wij om een DPIA uit te voeren.

Activiteit 8

Omschrijving activiteit 8

Ten behoeve van de Very High Readiness Joint Task Force (hierna: VJTF) voorbereiding wil de Intelligence, Surveillance and Reconnaissance Division (hierna: ISRD) van het Commando Luchtmacht (hierna: CLSK) informatie van het internet verzamelen en verwerken door middel van een scraper. De scraper is ontwikkeld door het bedrijf Tardis Research. Tardis Research is een softwarebedrijf dat zich heeft gespecialiseerd in big data analysis solutions. Omdat er een grote hoeveelheid aan mogelijk nuttige informatie op het (openbare) internet staat die een bijdrage kan leveren aan de besluitvorming, is deze behoefte ontstaan. De besluitvorming ziet dan met name toe op de vraag of er krijgsmachtspersoneel in het kader van de VJTF moeten worden uitgezonden en op welke wijze ze hierop moeten voorbereiden. De scraper doorzoekt hiervoor openbare bronnen met het doel om te duiden hoe situaties - bijvoorbeeld aan de grenzen van conflictgebieden - zich ontwikkelen.

Deze informatie uit openbare bronnen bestaat onder andere sociale media en fora (bijvoorbeeld Reddit). Uit die informatie wordt aan de hand van bepaalde factoren beoordeeld hoe betrouwbaar de informatie is. Er is geen interesse in het verwerken van persoonsgegevens. De intentie van deze activiteit ligt op het vergaren van bruikbare informatie ter ondersteuning van de besluitvorming en de informatiebehoefte. Het verwerken van persoonsgegevens (als 'bijvangst') is waarschijnlijk niet te voorkomen. Zowel een gebruikersnaam (ook indien het een pseudoniem is) als de informatie in een openbaar gedeeld bericht kunnen gewone - en in uitzonderlijke gevallen bijzondere - persoonsgegevens bevatten. Omdat handmatig doorzoeken van de grote hoeveelheid aan data die op internet beschikbaar is een bewerkelijke taak is, kan hiervoor een scraper worden ingezet. De scraper kan door middel van geautomatiseerde zoektermen uit een aanzienlijke hoeveelheid bulk data relevante informatie filteren.

Deze activiteit is naar aanleiding van de onderzoeken en commotie rondom het Land Information Manoeuvre Centre (hierna: LIMC) en het daaropvolgende onderzoek naar activiteiten die mogelijk knellen met de Algemene verordening gegevensbescherming (hierna: AVG) stopgezet.

Zoals gezegd is de intentie niet om persoonsgegevens te verwerken, maar komen deze als 'bijvangst' bij de openbaar gepubliceerde informatie waarschijnlijk altijd wel mee. Om de betrouwbaarheid van de informatie te valideren wil ISRD het liefst zowel de informatie als de bron controleren. De nadruk ligt hierbij overigens op het valideren van de informatie. Op het moment

dat duidelijk is dat een bepaald Twitteraccount vaak bruikbare informatie deelt, dan wordt dit account onthouden en is hervalideren vaak niet meer nodig. De ratio achter deze activiteit is gelegen in het feit dat er een informatiebehoefte bestaat om informatie in de context van de situatie tussen gereedstellen en een artikel 100 brief (inzet). Het mechanisme waarbij de Militaire Inlichtingen en Veiligheidsdienst (hierna: MIVD) aan deze informatiebehoefte voldoet is op dat moment namelijk nog niet in werking getreden. De informatiebehoefte ziet met name toe op dat de operationele eenheden. Zij moeten weten hoe een situatie in het buitenland zich ontwikkeld, hoe groot de kans is op inzet en wat in dat gebied is te verwachten qua (hoeveelheid) materieel en techniek van de potentiële tegenstander. Ook bij een oefening gaat het mechanisme niet af en is het CLSK verantwoordelijk voor de eigen informatievoorziening.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van CLSK, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub m AOD bepaalt dat het Ministerie van Defensie de Commandant Luchtstrijdkrachten als verantwoordelijke kent.

Artikel 14 AOD bepaalt over de Commandant Luchtstrijdkrachten het volgende:

“De Commandant Luchtstrijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Luchtstrijdkrachten;*
- b. de gereedstelling en instandhouding van de luchtstrijdkrachten;*
- c. het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*

- d. *het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Luchtstrijdkrachten;*
- e. *de advisering op het gebied van militair luchtoptreden.”*

Artikel 26 AOD bepaalt dat de Commandant Luchtstrijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Luchtstrijdkrachten 2018

Artikel 10 van het Subtaakbesluit Commando Luchtstrijdkrachten 2018 (hierna: subtaakbesluit) kent de volgende taken toe aan de Directie Operaties:

“De Directie Operaties staat onder leiding van de Directeur Operaties die is belast met:

- a. *het, met inachtneming van de aanwijzingen en de richtlijnen van Commandant Luchtstrijdkrachten, geven van ambtelijke leiding aan de Directie Operaties;*
- b. *het borgen van de operationele geoefendheid en inzetbaarheid binnen het Commando Luchtstrijdkrachten. Hiertoe behoort onder meer het opstellen of verfijnen en bewaken van operationele kwaliteitsnormen, en het periodiek toetsen van de mate waarin daaraan wordt voldaan en het initiëren van de benodigde corrigerende acties;*
- c. *mede gelet op de huidige taken van de Directie Operaties, het, al dan niet als formerend Operationeel Commando, in opdracht en onder verantwoordelijkheid van de Commandant der Strijdkrachten uitvoeren van coördinerende activiteiten ten behoeve van operaties;*
- d. *het adviseren van de Commandant Luchtstrijdkrachten over operatie gerelateerde zaken in het kader van de doctrine en Luchtvaarteseisen;*
- e. *het ondersteunen van de operationele eenheden bij het uitvoeren van hun operationele taken;*
- f. *het borgen van de kennis voor het (mede) leiden en/of ondersteunen van een joint of combined luchtoperatie boven het squadronniveau;*
- g. *het afstemmen van operaties en andere joint activiteiten met de andere betrokkenen en de operatiecentra;*
- h. *het borgen van de kwaliteit van de voor de missie essentiële operationele elementen binnen het Commando Luchtstrijdkrachten waaronder gevechtsleiding, luchtverkeersbeveiliging, brandweer, elektronische oorlogvoering en operationele inlichtingen;*
- i. *het binnen het Commando Luchtstrijdkrachten optreden als aanspreekpunt voor de Directie Operaties van de Defensiestaf;*
- j. *het optreden als beveiligingscoördinator van het Commando Luchtstrijdkrachten;*

k. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Luchtstrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;

l. de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de Directie Operaties."

Op grond van de taakstelling die uit artikel 10 sub b, d, f, h en k is het voorzien in de informatiebehoefte en tactisch-operationeel adviseren de interne taak van CLSK.

Toepassingsbereik AVG

De AVG is van toepassing als de activiteit binnen het materieel en territoriaal toepassingsgebied van de AVG valt.

Materieel toepassingsbereik

Op het moment dat een scraper wordt ingezet is het doel daarvan uitdrukkelijk niet om persoonsgegevens te verwerken. Er worden wel persoonsgegevens als 'bijvangst' verwerkt. Ook daarop is de AVG van toepassing. Deze (potentiële) activiteit valt dus binnen het materieel toepassingsbereik van de AVG.

Territoriaal toepassingsbereik

Als de potentiële activiteit wordt uitgevoerd verwerkt ISRD persoonsgegevens onder verantwoordelijkheid van de Minister van Defensie. Deze persoonsgegevens worden tevens in Nederland verwerkt. Op basis daarvan valt de potentiële activiteit binnen het territoriaal toepassingsbereik van de AVG.

177

De AVG is dus van toepassing op deze potentiële activiteit.

Beoordeling activiteit

Artikel 5 AVG bepaalt aan welke beginselen de verwerking van persoonsgegevens moet voldoen. Er is reeds een Data Protection Impact Assessment (hierna: DPIA) uitgevoerd bij het Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando (hierna: JISTARC) op (het gebruik van) de tooling van Tardis. Uit deze DPIA is gebleken dat een grondslag voor het verwerken van persoonsgegevens ontbreekt. De Functionaris Gegevensbescherming (hierna: FG) heeft derhalve de DPIA en daarmee de verwerking afgewezen in haar appreciatie. Om die reden vindt de activiteit daarom geen doorgang en gaan we niet in op alle beginselen van artikel 5 AVG. Om te bevestigen dat er geen grondslag toetsen we enkel de rechtmatigheid.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens mogen verwerkt als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd. De taak moet daarnaast duidelijk en specifiek genoeg zijn omschreven dat het voor de betrokkene helder is dat er persoonsgegevens worden verwerkt en voor welk doel. Het is bovendien enkel toegestaan om de persoonsgegevens te verwerken die noodzakelijk zijn om die taak te vervullen.

Uit het subtaakbesluit volgt geen interne taaktoebedeling die ziet op het inzetten van een scraper om (informatie rondom) ontwikkelingen te verzamelen en daarbij persoonsgegevens als bijvangst te verwerken door CLSK (en in het verlengde daarvan ISRD). Daarnaast valt een subtaakbesluit niet als publieke taak te kwalificeren en is de taakomschrijving an sich onvoldoende specifiek omschreven, waardoor niet voorzienbaar is dat het noodzakelijk is om persoonsgegevens te verwerken om de taak uit te voeren. Daarnaast is het subtaakbesluit een ministeriële regeling, waardoor het – zelfs als op basis van de taakomschrijving voldoende voorzienbaar is dat er persoonsgegevens worden verwerkt – geen bevoegdheid kan scheppen in de zin van artikel 6 lid 1 sub e AVG. Om een dusdanige bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een AOD, en in het verlengde daarvan een subtaakbesluit, missen deze rechtskracht.

178

Een publieke taak en bevoegdheid om in het kader van het algemeen belang persoonsgegevens te verwerken door middel van een scraper, al dan niet als bijvangst, ontbreekt. Dat de intentie niet is gericht op het verwerken van persoonsgegevens maakt deze lezing niet anders. Om een taak én bevoegdheid te creëren is een wet in de formele zin vereist en een subtaakbesluit (materiële wetgeving) mist deze rechtskracht.

Gerechtvaardigd belang

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak. In het geval dat het om een typisch bedrijfsmatige handeling van een overheidsinstantie

gaat is dit wel een mogelijkheid.⁹² Daarbij moet het verwerken van persoonsgegevens noodzakelijk zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. Een beroep op het gerechtvaardigd belang is voor overheidsorganen niet mogelijk wanneer de verwerking plaatsvindt in het kader van de uitoefening van haar taken.⁹³

Een voorbeeld van een typisch bedrijfsmatige handeling van een overheidsinstantie is het beveiligen van gebouwen. Dit wijkt namelijk niet af van private organisaties die hun eigen gebouwen en eigendommen op grond van het gerechtvaardigd belang beveiligen. Bij deze potentiële activiteit gaat het om het inzetten van een scraper om informatie uit openbare bronnen te verzamelen. Met deze informatie worden ontwikkelingen van situaties geduid, ter ondersteuning van de besluitvorming. Hierbij is het onvermijdelijk is om geen persoonsgegevens te verwerken. Het inzetten van een scraper is volgens ons in geen geval aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie. Een beroep op het gerechtvaardigd belang slaagt daarom niet.

Mogelijke knelpunten

ISRD van CSLK voert deze potentiële activiteit niet uit omdat er waarschijnlijk geen grondslag is voor het verwerken van persoonsgegevens. Daarbij zijn enkele mogelijke knelpunten gesignaleerd.

179

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Voor de verwerking van persoonsgegevens in het kader van de inzet van een scraper ligt de grondslag van artikel 6 lid 1 sub e AVG, vervulling van een taak van algemeen belang, voor de hand. Hiervoor is het noodzakelijk dat de taak aan de verwerkingsverantwoordelijke, in deze Defensie, zijn opgedragen bij Europees of Nederlands recht. Het doel van de verwerking moet daarbij duidelijk zijn af te leiden uit de	Indien het noodzakelijk wordt geacht om ter ondersteuning van de (algemene) informatiebehoefte en daarmee de besluitvorming, openbaar toegankelijke informatie – en persoonsgegevens als mogelijke ‘bijvangst’ - te verwerken, moet hiervoor een formeel wettelijke taak worden gecreëerd door de wetgever. Deze taak moet dan dusdanig helder zijn geformuleerd dat het voor de betrokkene is af te leiden welke persoonsgegevens worden verwerkt. Gelet op de beginselen van

⁹² Zie Memorie van toelichting op AVG, Kamerstukken II 2017/18, 2034 851, nr. 3, p. 37

⁹³ Zie Tekst & Commentaar Algemene verordening gegevensbescherming, p. 92.

	<p>taakomschrijving. De grondslag om persoonsgegevens te verwerken ten behoeve van deze activiteit lijkt te ontbreken.</p>	<p>rechtmatigheid, transparantie en doelbinding is enkel een formele wetgeving afdoende om tot een geldige grondslag in de zin van artikel 6 lid 1 sub e AVG te komen.</p>
<i>Organisatorisch</i>		
2.	<p>Het is de verwachting dat de MIVD te weinig capaciteit en daarmee gewenste én vereiste slagkracht heeft op het moment dat het nodig is. In het geval van een conflict is de rangorde van ondersteuning volgens de respondent als volgt:</p> <ol style="list-style-type: none"> 1. Politieke besluitvorming; 2. Commandant der Strijdkrachten (hierna: CDS); 3. Operationele Commando's (hierna: OPCO's, waaronder CLSK). <p>Dit levert mogelijk problemen op. Het is waarschijnlijk 'te laat' als er pas informatie wordt verzameld op het moment dat de vliegtuigen al de lucht in moeten. Bovendien ontstaat daarmee een informatieachterstand ten opzichte van de tegenstander.</p>	<p>De MIVD en AIVD opereren voor het uitvoeren van inlichtingenactiviteiten onder de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv2017). Het ISRD is geen (althans niet formeel in de zin van de wet) inlichtingendienst en valt onder het Commando Luchtstrijdkrachten. Derhalve kan ISRD niet onder de Wiv2017 met bijbehorende kaders en systemen van toezicht opereren.</p> <p>De MIVD is als onderdeel van Defensie verweven met de krijgsmacht, met de gezaghebbende inlichtingenpositie om relevante en betrouwbare informatie te vergaren, verwerken en analyseren, om hiermee beslissend te kunnen handelen op strategisch niveau tot inzet van operationeel-tactische eenheden.</p> <p>Naast deze primaire taakstelling ondersteunt de MIVD eveneens de krijgsmachtonderdelen met inlichtingenopleidingen en innovatie.</p> <p>Het lijkt een onmogelijkheid om alle (relevante) informatie uit te wisselen, of mee te nemen naar het eigen krijgsmachtonderdeel. Een oplossing voor informatieachterstand(en) op het gebied van informatie gestuurd optreden (hierna: IGO) tussen krijgsmachtonderdelen is hiermee derhalve niet gegeven.</p>

		<p>De respondenten spreken de wens uit om de activiteiten onder de AVG uit te voeren. Zodat zij zelf in een eerder stadium informatie kunnen verzamelen, zonder afhankelijk te zijn van de MIVD. Dit zou betekenen dat er een formeel wettelijke grondslag moet worden gecreëerd. Momenteel ontbreekt namelijk een grondslag om bij deze activiteit zelf persoonsgegevens te verwerken.</p> <p>Bovendien, ervaring leert dat voor inzet van bijzondere bevoegdheden conform de Wiv2017 vaak veel tijd en ruimte nodig is, wat niet aansluit bij de snelheid van het militair operationele niveau.</p>
--	--	---

Conclusie

Hoewel de activiteit niet gaande is, zijn er voor eventueel toekomstig gebruik mogelijk knelpunten geconstateerd die maken dat de activiteit in de gewenste vorm waarschijnlijk niet kan doorgaan. Op dit moment is er geen verwerkingsgrondslag aanwezig die het mogelijk maakt om persoonsgegevens te verwerken. Dezelfde conclusie volgt ook uit de DPIA die is uitgevoerd door JISTARC op de scraper van Tardis. Hoewel er geen intentie is om persoonsgegevens te verwerken, vindt dit onoverkomelijk plaats in de vorm van bijvangst.

Omdat de rechtmatigheid om persoonsgegevens te verwerken ontbreekt door het missen van een grondslag krijgt deze activiteit de kleur rood.

Activiteit 9A

Omschrijving activiteit 9A

Deze activiteit vindt (nog) niet plaats.

Het Korps Mariniers van het Commando Zeestrijdkrachten (hierna: CZSK) heeft de wens om gebruik te maken van een geïntegreerd mobiel interceptieplatform (hierna: GMI). Het GMI verzamelt en verwerkt data door middel van Cyber and Electromagnetic Activities (hierna: CEMA). Hiermee kunnen onder andere radio-, wifi- en Bluetoothsignalen worden verwerkt. Het doel hiervan is de Operational Security (hierna: OPSEC) en de Digital Force Protection zeker te stellen en om de eigen defensiemedewerkers bewust te maken van de risico's en consequenties van de verspreiding van informatie.⁹⁴ Met een GMI kunnen kort gezegd interne en externe risico's in kaart worden gebracht.

Onder interne risico's worden signalen verstaan die afkomstig zijn van mobiele apparaten van de eigen mariniers en die getraceerd kunnen worden door een mogelijke vijand. Inzet van een GMI zorgt ervoor dat duidelijk in kaart wordt gebracht of er interne signalen worden uitgezonden. Ook kan worden bekeken van wie die interne signalen afkomstig zijn. Als een dergelijke signalering risico's voor de veiligheid van de betreffende eenheid met zich meebrengt kan CZSK, op basis van die signalering, maatregelen treffen om deze risico's te mitigeren.

Onder externe risico's worden signalen verstaan die afkomstig zijn van mobiele apparaten die zich buiten, maar in de nabijheid van, de betreffende eenheid bevinden. Inzet van een GMI zorgt ervoor dat in kaart wordt gebracht welke signalen er worden uitgezonden, waar die signalen van afkomstig zijn en of wel of geen potentieel risico bestaat voor de veiligheid van de betreffende eenheid. Op basis van die signalering kan CZSK maatregelen treffen om de risico's te mitigeren.

Met het gebruik van een GMI kunnen persoonsgegevens worden verwerkt van de eigen mariniers en van derden die niet aan Defensie zijn gelieerd en zich binnen het ontvangstbereik van het GMI bevinden. Om onderscheid aan te brengen in de verwerking van de persoonsgegevens van deze twee groepen en ter bevordering van de leesbaarheid van dit document, worden de mariniers en andere medewerkers van Defensie hierna aangeduid als 'internen' en de derden die niet gerelateerd zijn aan Defensie als 'externen'.

⁹⁴ Onder te verzamelen en verwerken data wordt data verstaan die afkomstig is van de signalen die worden uitgezonden door de mobiele apparaten die de mariniers enerzijds en externen anderzijds bij zich dragen.

In deze uitwerking van activiteit 9A richten wij ons op de verwerking van persoonsgegevens van internen. In de uitwerking onder activiteit 10B gaan wij in op de verwerking van persoonsgegevens van externen.

Gebruik geïntegreerd mobiel interceptieplatform (afgekort: GMI)	
Wie?	Commando Zeestrijdkrachten onder verantwoordelijkheid van de Minister van Defensie.
Wat?	Constateren signalen (telefoon, radio, etc.) in de kijkomgeving en het uitlezen van die signalen, waarbij mogelijk persoonsgegevens worden verwerkt.
Waar?	Wereldwijd. De scope van dit onderzoek beperkt zich tot gebruik op Nederlands grondgebied en op schepen en luchtvaartuigen die zich in Nederlandse wateren, respectievelijk het Nederlandse luchtruim, bevinden.
Wanneer?	Tijdens algemene gereedstelling (er is dan geen sprake van een regeringsbesluit/mandaat).
Waarom?	Door de omgeving in kaart te brengen kan de eenheid beter beschermd worden.
Hoe?	Opvangen signalen door middel van een antenne, het omzetten van de opgevangen signalen in een voor mensen leesbare vorm op de standalone laptop, het raadplegen van de gegevens die uit de signalen kunnen worden afgeleid.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van het CZSK zoals deze uit verschillende wet- en regelgeving blijken.

Algemeen organisatiebesluit Defensie 2021

Artikel 12 van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) geeft de volgende taak aan de Commandant Zeestrijdkrachten:

“De Commandant Zeestrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Zeestrijdkrachten;*

- b. De gereedstelling en instandhouding van de zeestrijdkrachten;
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;
- d. Het binnen de gestelde normen en kader uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Zeestrijdkrachten;
- e. Het beheer van de Kustwacht Nederland en de Kustwacht Caribische Gebied;
- f. De advisering op het gebied van militair maritiem optreden."

Het beoogde gebruik van het GMI vindt plaats om digitale verkenningen te kunnen uitvoeren om de veiligheid van de mariniers te kunnen waarborgen. Door eventuele risico's – zoals uitgaande mobiele signalen van opvarenden – vroegtijdig in kaart te brengen, kan CZSK tijdig daarop anticiperen. Het uitvoeren van digitale verkenningen kan – met een ruime interpretatie – als middel worden gezien om de zeestrijdkrachten in stand te houden, zoals genoemd in artikel 12, aanhef en onder b, AOD.

Subtaakbesluit Commando Zeestrijdkrachten 2010

Artikel 26 AOD bepaalt dat er subtaakbesluiten kunnen worden vastgesteld. CZSK beschikt over het Subtaakbesluit Commando Zeestrijdkrachten 2010 (hierna: subtaakbesluit). Dit subtaakbesluit voorziet de verschillende onderdelen binnen CZSK van een nadere taakomschrijving. Artikel 5 van het subtaakbesluit geeft de volgende taak aan de Directie Operaties:

"De directie Operaties staat onder leiding van de directeur Operaties die is belast met:

- a. *het met inachtneming van de opdracht, planningskaders en (functionele) richtlijnen van de Commandant Zeestrijdkrachten geven van leiding aan de directie Operaties;*
- b. *het ontwikkelen en onderhouden van maritiem-expeditionair vermogen in al zijn facetten;*
- c. *het ontwikkelen en onderhouden van maritieme doctrines en tactieken;*
- d. *het aanbrengen en behouden van de geoefendheid van enkelvoudige eenheden, samengestelde eenheden en een 'deployable' staf;*
- e. *mede gelet op de taken van het Defensie Operatie Centrum, het, al dan niet als formerend Operationeel Commando, in opdracht en onder verantwoordelijkheid van de Commandant der Strijdkrachten uitvoeren van coördinerende activiteiten t.b.v. operaties;*
- f. *het coördineren van de ondersteuning van eenheden die worden ingezet door de Commandant der Strijdkrachten, dan wel de Belgische Chief of Defense voor zover die inzet in binationaal verband en via de organisatie van de Admiraal Benelux wordt aangestuurd;*

- g. *de operationele planning van operaties voorafgaande aan maar ook tijdens en na de operaties ten behoeve van het Defensie Operatie Centrum en het Belgische Center of Operations;*
- h. *het geven van leiding aan de Dienst der Hydrografie en in dat kader uitvoeren van hydrografische, oceanografische en meteorologische ondersteuning bij militair optreden met daarnaast systematisch zeebodemonderzoek en nautische kartering overeenkomstig internationale verdragen;*
- i. *het ontwikkelen en onderhouden van functionele richtlijnen – ten aanzien van het eigen terrein van verantwoordelijkheid – voor de gehele CZSK-organisatie;*
- j. *het binnen het Commando Zeestrijdkrachten optreden als aanspreekpunt voor de directeur van de directie Operaties van de Defensiestaf;*
- k. *het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;*
- l. *de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de directie Operaties."*

Het beoogde gebruik van het GMI kan mogelijk worden geschaard onder de uitvoering van een van de taken uit artikel 12 sub b AOD of artikel 5, sub b en c van het subtaakbesluit.

185

Toepassingsbereik AVG

Vaststellen scope activiteit in het kader van het onderzoek

Tijdens het interview is naar voren gekomen dat de inzet van een GMI onder uiteenlopende omstandigheden en op diverse locaties mogelijk moet zijn. Dit zorgt ervoor dat het Korps Mariniers, bij de inzet van een GMI, ook te maken kan krijgen met internationale en buitenlandse wet- en regelgeving voor de verwerking van (persoons)gegevens. In dit AVG-onderzoek beperken wij ons tot de inzet van een GMI op Nederlands grondgebied en op schepen die zich in Nederlandse wateren bevinden.

Dit onderzoek richt zich op informatie gestuurd optreden door eenheden van het Ministerie van Defensie ten tijde van algemene gereedstelling. Omdat aan specifieke gereedstelling en aan inzet een regeringsbesluit of een besluit van de Minister van Defensie ten grondslag ligt, waaruit specifieke bevoegdheden voor de eenheden kunnen voortvloeien, wordt informatie gestuurd optreden ten tijde van specifieke gereedstelling en inzet buiten beoordeling gelaten in dit onderzoek.

Materieel toepassingsbereik

Respondent heeft aangegeven dat het GMI verscheidene signalen kan opvangen en verwerken, waaronder telefoonsignalen, radiosignalen, wifisignalen en Bluetoothsignalen. Wanneer de antenne van het GMI een signaal opvangt, wordt dit signaal verwerkt op zo'n manier dat het voor mensen begrijpelijk en leesbaar is. Deze begrijpelijke en leesbare versie van het signaal kan vervolgens worden afgelezen van de laptop die met het GMI verbonden is.

Op basis van een ontvangen telefoonsignaal kan mogelijk worden afgeleid wie de eigenaar en/of gebruiker van het toestel is en wat hij of zij ermee heeft gedaan. Het opgevangen signaal kan namelijk een hoop metadata prijsgeven, welke data herleidbaar kan zijn tot een individu. Het kan dan bijvoorbeeld gaan om de unieke MAC-adressen en locatiegegevens die kunnen worden gecombineerd met tijdstip en plaats, en mogelijke wifi- en Bluetooth namen van persoonlijke hardware. Wanneer een GMI wordt gebruikt kunnen er, afhankelijk van in hoeverre de signalen worden uitgelezen, persoonsgegevens worden verwerkt.

Voor gebruik van een GMI ten tijde van specifieke gereedstelling en inzet kan op grond van de Regeling gegevensbescherming militaire operaties (hierna: RGMO) (gedeeltelijk) worden afgeweken van de AVG. Dit gebeurt door middel van een regeringsbesluit dat, voorafgaand aan de specifieke gereedstelling of inzet, wordt opgesteld door de Minister van Defensie. Ten tijde van algemene gereedstelling, waarbij de krijgsmacht zich onder meer bezighoudt met algemene trainingsdoeleinden, is er geen sprake van een regeringsbesluit waarin gedeeltelijk kan worden afgeweken van de AVG. De AVG en de UAVG zijn dus onverkort van toepassing op het gebruik van een GMI ten tijde van algemene gereedstelling.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

Een GMI kan ook worden gebruikt buiten Nederland en buiten de Europese Economische Ruimte (hierna: EER). Zelfs wanneer met het GMI persoonsgegevens worden verwerkt, bijvoorbeeld op een marineschip dat zich in internationale wateren bevindt, is de AVG op deze verwerking van persoonsgegevens van toepassing. Zoals ook hierboven in de scopebepaling van deze activiteit is toegelicht, beperken wij ons tot het gebruik van een GMI op Nederlands grondgebied en op schepen die zich in Nederlandse wateren bevinden.

De AVG is dus van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens verwerkt mogen worden als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd waarbij het voor de betrokkene duidelijk moet zijn dat er persoonsgegevens worden verwerkt. Bovendien is het enkel toegestaan om persoonsgegevens op basis van deze grondslag te verwerken als het noodzakelijk is voor de vervulling van de publieke taak.

187

Uit overweging 45 van de AVG volgt dat de verwerking voor een succesvol beroep op artikel 6 lid 1 sub c AVG of artikel 6 lid 1 sub e AVG een grondslag moet hebben in een Unierechtelijke of lidstaatrechtelijke bepaling. Overweging 41 van de AVG voegt daaraan toe dat de rechtsgrond of wetgevingsmaatregel evenwel duidelijk en nauwkeurig moet zijn, en de toepassing daarvan voorspelbaar moet zijn voor degenen op wie deze van toepassing is.

Daarnaast bepaalt artikel 10 Gw dat een overheidsinstantie zich in beginsel niet mag inmengen in de persoonlijke levenssfeer van een burger, tenzij een wet in formele zin hiervoor een grondslag biedt én die wet regels stelt voor het beschermen van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens.

Dit brengt met zich mee dat de taak van algemeen belang ook moet voortvloeien uit een Unierechtelijke of lidstaatrechtelijke bepaling. Onder het kopje 'taakomschrijving' hebben wij opgemerkt dat deze activiteit volgens ons mogelijk geschaard kan worden onder een van de taken uit artikel 12 sub b AOD of artikel 5, sub b en c van het subtaakbesluit. Wij zijn echter van mening dat het AOD en het subtaakbesluit niet als grondslag kunnen dienen voor de verwerking van persoonsgegevens bij deze activiteit, omdat het AOD en

subtaakbesluit niet kunnen worden aangemerkt als lidstaatrechtelijke bepalingen met formele rechtskracht. Wij zijn daarnaast van mening dat uit de taakomschrijving onvoldoende voorzienbaar is dat er persoonsgegevens kunnen worden verwerkt met betrekking tot deze activiteit.

Respondent heeft aangegeven dat het in de informatiesamenleving noodzakelijk is om digitaal de omgeving te kunnen verkennen om risico's voor de eenheid vroegtijdig op te sporen en daarop te kunnen anticiperen.

Voorbeeld: met het GMI kan men waarnemen of er bijvoorbeeld verdachte wifisignalen worden aangeboden in de nabijheid van een marineschip. Bepaalde organisaties beschikken over hetzelfde wifinetwerk in iedere vestiging (bijvoorbeeld: McDonalds). Wanneer een marinier zijn mobiele telefoon al eens eerder heeft verbonden met het wifinetwerk bij de McDonalds, bestaat de kans dat zijn telefoon ook automatisch met het wifinetwerk verbindt van de McDonalds in een andere stad of in een ander land. Op zee kan een piratenschip bijvoorbeeld het netwerk van de McDonalds nabootsen, waardoor de telefoons van de mariniers automatisch met dat netwerk verbinden, met alle gevolgen van dien. Gebruik van een GMI kan voorkomen dat een dergelijk risico zich verwezenlijkt, door vroegtijdig het netwerk op zee te signaleren en daarop te anticiperen.

Respondent heeft vanuit het perspectief van CZSK duidelijk gemaakt waarom het voor CZSK noodzakelijk is om een GMI in te zetten ten tijde van algemene gereedstelling. Ondanks de door CZSK gehanteerde definitie van het begrip 'noodzaak', zijn wij van mening dat deze definitie zeer waarschijnlijk niet overeenkomt met de definitie van het noodzakelijkheidsbegrip uit de AVG. Om te kunnen spreken van noodzakelijkheid in het kader van de AVG, is het van belang dat er geen lichtere middelen voorhanden zijn om hetzelfde doel te bereiken (subsidiariteit). Mogelijk kan door gebruik van minder ingrijpende middelen worden voorkomen dat mariniers ongewenst signalen met mobiele apparaten uitzenden. Onderzocht zou kunnen worden of eenheden ook voldoende worden beschermd door het creëren van bewustwording door middel van trainingen, opleidingen of interne voorlichtingscampagnes. Een andere mogelijkheid is om aan mariniers toestellen te verstrekken van Defensie, die bijvoorbeeld op afstand kunnen worden uitgeschakeld, in samenhang met het verbod op het meebrengen van persoonlijke digitale apparaten.

Wij zijn dan ook van mening dat een beroep op het algemeen belang geen kans van slagen heeft.

Gerechtvaardigd belang

Artikel 6 lid 1 sub f AVG bepaalt dat de verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De laatste volzin van artikel 6 lid 1 sub f AVG voegt daaraan toe dat overheidsinstanties in het kader van de uitoefening van hun taken geen beroep kunnen doen op artikel 6 lid 1 sub f AVG.

In hoofdstuk 5 van dit rapport hebben wij uiteengezet dat een beroep op het gerechtvaardigd belang door overheidsinstanties alleen mogelijk is voor typisch bedrijfsmatige handelingen van die overheidsinstanties. In de literatuur en rechtspraak is het begrip 'typisch bedrijfsmatige handeling' echter onvoldoende uitgewerkt. Hierdoor kunnen wij niet beoordelen in hoeverre deze activiteit als typisch bedrijfsmatige handeling kan worden aangemerkt. Er is hierbij dus sprake van een grijs gebied. Gezien de specialistische apparatuur en beoogde toepassing ervan is ons inziens geen sprake van typisch bedrijfsmatige handelingen bij deze activiteit.

Daarbij moet het verwerken van persoonsgegevens noodzakelijk zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dit belang prevaleren boven die van de betrokkene. Zoals wij hiervoor onder het kopje 'algemeen belang' al hebben toegelicht, lijkt het erop dat niet aan het noodzakelijkheidsvereiste in de zin van de AVG wordt voldaan. Voor zover Defensie van mening is dat wel aan het noodzakelijkheidsbeginsel wordt voldaan, is het van belang dat er voorafgaand aan het verwerken van persoonsgegevens een Data Protection Impact Assessment (hierna: DPIA) wordt uitgevoerd, waarin de reikwijdte van het gebruik wordt vastgelegd en per type verwerking wordt vastgelegd wat de risico's zijn en hoe groot die risico's zijn.

Gelet op het bovenstaande kan CZSK bij deze beoogde activiteit geen beroep doen op verwerking van persoonsgegevens op grond van een gerechtvaardigd belang uit artikel 6 lid 1 sub f AVG.

Concluderend merken wij op dat CZSK niet over een grondslag beschikt voor het verwerken van persoonsgegevens in deze beoogde activiteit.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het ontbreken van een wettelijke grondslag voor het gebruik van een GMI.	Het creëren van een formeel wettelijke grondslag, waaruit duidelijk kan worden afgeleid dat er een noodzaak bestaat om persoonsgegevens te verwerken. De verwerking van persoonsgegevens (ook als bijvangst) dient namelijk voorzienbaar te zijn bij wet. Een generieke taakomschrijving, waaruit bijvoorbeeld blijkt dat de Commandant Zeestrijdkrachten zorg dient te dragen voor het waarborgen van de veiligheid van de mariniers, is in dit licht onvoldoende.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

190

Respondent heeft aangegeven dat mariniers, voorafgaand aan de inzet van een GMI, zullen worden geïnformeerd over de mogelijkheid dat hun persoonsgegevens kunnen worden verwerkt door het opvangen van de signalen die afkomstig zijn van hun mobiele apparaten.

Om ervoor te zorgen dat de informatievoorziening in overeenstemming is met de AVG, dient CZSK te zorgen voor een herziening van de privacyverklaring, door daarin de informatie toe te voegen zoals vermeld in artikel 13 AVG, over de gegevensverwerking door het GMI. De mariniers dienen deze informatie, op het moment van het verkrijgen van de persoonsgegevens door CZSK, te ontvangen.⁹⁵

Uitzonderingen op de informatieplicht

Artikel 13, 14 en 23 AVG en artikel 41 UAVG kennen enkele uitzonderingen op de informatieplicht in het kader van behoorlijkheid en transparantie.

⁹⁵ Zie artikel 13 lid 1 AVG.

De uitzondering in artikel 13 ziet op de situatie waarin persoonsgegevens rechtstreeks van betrokkene worden verzameld en betrokkene reeds over de informatie zoals genoemd in artikel 13 AVG beschikt. Bij het verzamelen van eventuele persoonsgegevens door middel van het GMI wordt de informatie ook rechtstreeks van betrokkene verkregen.⁹⁶ Echter is ons niet gebleken dat betrokkenen reeds over alle te verstrekken informatie beschikken, zoals genoemd in artikel 13 AVG. De uitzondering op de informatieplicht in artikel 13 AVG is daarom niet van toepassing.

De uitzonderingen in artikel 14 AVG zien op de situatie waarin persoonsgegevens niet rechtstreeks zijn verkregen van de betrokkene. Bij het verzamelen van eventuele persoonsgegevens door middel van het GMI wordt informatie juist wel direct van betrokkenen verkregen. De uitzonderingen op de informatieplicht in artikel 14 AVG zijn daarom niet van toepassing.

Op grond van artikel 23 AVG en het overeenkomstige artikel 41 UAVG kan een uitzondering worden gemaakt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

- a) de nationale veiligheid
- b) landsverdediging
- c) de openbare veiligheid

Respondent gaf aan dat met het GMI eventuele signalen van mobiele telefoons van mariniers kunnen worden gesignaleerd, met als doel om bewustwording te creëren onder de mariniers, en daarmee de veiligheid van de mariniers of opvarenden te waarborgen. Alhoewel kan worden gesteld dat dit doel indirect een bijdrage zou kunnen leveren aan de waarborging van de nationale veiligheid, landsverdediging en de openbare veiligheid, zijn wij van mening dat deze activiteit geen noodzakelijke en evenredige maatregel is ter waarborging van deze belangen. Bovendien zijn ons geen uitzonderingen in Unierechtelijke of lidstaatrechtelijke bepalingen gebleken op grond waarvan CZSK, bij de verwerking van persoonsgegevens bij deze activiteit, een uitzondering kan maken op de informatieplicht.

Concluderend merken wij op dat aan het beginsel van behoorlijkheid en transparantie niet wordt voldaan.

⁹⁶ Vergelijk Richtsnoeren inzake transparantie overeenkomstig Verordening (EU)2016/679 van WG29, p. 16, paragraaf 26.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
2.	In het kader van de informatieplicht uit artikel 13 AVG is het van belang mariniers te informeren over de eventuele verwerking van hun persoonsgegevens door een GMI.	In eenvoudige en duidelijke taal omschrijven van het doel van de verwerking van persoonsgegevens door een GMI, wat er met de gegevens gebeurt en de overige informatie die wettelijk verstrekt moet worden op basis van artikel 13 AVG.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel moet worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

Respondent heeft aangegeven dat het voor het waarborgen van de veiligheid van de mariniers en andere medewerkers van Defensie van belang is om te weten of zij hun mobiele apparaten hebben uitgeschakeld, zodat zij vervolgens kunnen worden gewezen op de risico's die zij veroorzaken voor zichzelf en andere opvarenden.

192

Hoewel het gebruik van een GMI op het eerste gezicht een te verstrekend middel lijkt te zijn om dit doel te bereiken, zijn mogelijke alternatieven ook niet waterdicht. Ter illustratie:

- Mariniers kunnen worden gesommeerd om hun mobiele apparaten uit te schakelen en in te leveren aan het begin van de algemene gereedstelling. In de praktijk kunnen mariniers echter twee apparaten meenemen en een daarvan inleveren, zodat zij het andere apparaat nog wel stiekem kunnen gebruiken;
- Het controleren of er mobiele apparaten zijn ingeschakeld door gebruik te maken van een apparaat dat als bijvangst geen persoonsgegevens verwerkt, maar uitsluitend signalen constateert. De vraag is echter of het technisch mogelijk is om zo'n apparaat te ontwikkelen. Daarbij doet zich ook het risico voor dat de betreffende marinier niet kan worden geïdentificeerd, op het moment dat hij geen gehoor geeft aan het bevel om zijn mobiele apparaat alsnog uit te schakelen.
- Het Ministerie van Defensie kan ervoor kiezen om mariniers uitsluitend gebruik te laten maken van (geprepareerde) mobiele apparaten, welke eventueel op afstand beheerd en uitgeschakeld kunnen worden, indien de situatie daarom vraagt. Het risico hierbij is dat mariniers stiekem

alsnog een persoonlijk mobiel apparaat meenemen, welke eenmaal op het kamp kan worden gebruikt.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Respondent heeft aangegeven dat wanneer mariniers hun mobiele apparaat aan hebben staan, op basis van de metadata onderzocht kan worden wat de marinier met het betreffende apparaat heeft gedaan (zoals het versturen van een sms-bericht op een bepaald tijdstip) en van welke marinier het betreffende apparaat is (op basis van de locatiegegevens in combinatie met het IP-adres).

Mogelijke knelpunten		Aanbevelingen
Juridisch		
3.	Uit het onderzoek is ons niet gebleken dat Defensie reeds beschikt over protocollen, waarin bijvoorbeeld is vastgelegd wanneer diepgaander onderzoek naar een signaal wordt verricht.	In het kader van minimale gegevensverwerking verdient het aanbeveling om een protocol op te stellen waarin is vastgesteld wanneer een signaal als ongewenst of verdacht wordt aangemerkt en onder welke omstandigheden diepgaander onderzoek is toegestaan.
4.	Vooralsnog is het onbekend welke persoonsgegevens noodzakelijk zijn om het doel van het gebruik van een GMI te bereiken.	In het kader van minimale gegevensverwerking verdient het aanbeveling om in de gevallen waarbij diepgaander onderzoek naar metadata wordt gedaan, alleen die metadata te onderzoeken die noodzakelijk is om de identiteit van de betrokkene te achterhalen.

Mogelijke knelpunten		Aanbevelingen
Organisatorisch		
5.	Vooralsnog is het onbekend wat de gevolgen zijn op het moment dat een ongewenst digitaal signaal afkomstig van een mobiel apparaat van een marinier wordt gedetecteerd.	Op het moment dat een signaal van een marinier wordt gedetecteerd, kan er voor worden gekozen om eerst in algemene zin de mariniers nogmaals dringend te verzoeken hun mobiele apparaten uit te schakelen. Wordt het signaal bij een tweede scan nogmaals

		geconstateerd, dan kan bijvoorbeeld worden overgegaan tot nader onderzoek, waarbij ook persoonsgegevens worden verwerkt.
--	--	--

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Omdat metadata objectieve informatie is, zal van rechtswege aan het juistheidsbeginsel worden voldaan. Naast het feit dat de te verwerken gegevens juist moeten zijn, is het ook van belang om vast te stellen wat er met die gegevens gaat gebeuren. Respondent heeft aangegeven dat de verwerkte persoonsgegevens onder omstandigheden ook gekoppeld kunnen worden aan andere (persoons)gegevens.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren valt, dan moeten de persoonsgegevens worden gewist.

194

Respondent heeft aangegeven dat verwerkte persoonsgegevens niet langer zullen worden bewaard dan noodzakelijk, maar dit proces is nog niet nader is uitgewerkt.

Daarnaast heeft respondent aangegeven dat voor de verwerking van de persoonsgegevens een standalone laptop zal worden gebruikt die is verbonden met het GMI, waardoor van enige vorm van gegevensuitwisseling geen sprake is. Opmerking verdient dat respondent heeft aangegeven dat het GMI wordt ontwikkeld in samenwerking met de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO). Op de vraag of met TNO ook persoonsgegevens worden uitgewisseld, bijvoorbeeld om het apparaat te testen, antwoordde respondent negatief. Van enige vorm van gegevensuitwisseling lijkt dan ook geen sprake te zijn.⁹⁷

⁹⁷ Opmerking verdient dat respondent ook heeft aangegeven dat een GMI kan worden ingezet in vliegtuigen. Voor het technisch regelen van de stroomvoorziening moet dan worden samengewerkt met het Nederlandse Lucht- en Ruimtevaartcentrum (NLR). Volgens respondent worden daarbij geen persoonsgegevens uitgewisseld.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
6.	Vooralsnog ontbreken specifieke bewaartermijnen voor eventuele persoonsgegevens die bij het gebruik van een GMI worden verwerkt.	<p>Generieke bewaartermijnen vastleggen en een protocol opstellen waaruit blijkt op welke manier de vernietiging van de persoonsgegevens plaatsvindt.</p> <p>Ter illustratie: voor signalen die worden opgevangen door een GMI tijdens een trainingsmissie kan een bewaartermijn gehanteerd worden tot zes maanden na afloop van de trainingsmissie.</p> <p>Indien het noodzakelijk is om persoonsgegevens langer te bewaren, dienen er aanknopingspunten te worden vastgelegd in het protocol onder welke omstandigheden langer bewaren geoorloofd is.</p>

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

195

Respondent heeft aangegeven dat voor de beveiliging van de persoonsgegevens gebruik wordt gemaakt van een standalone laptop, die verbonden kan worden met het GMI, en uitsluitend toegankelijk is voor daarvoor geautoriseerde personen. Daarnaast heeft respondent aangegeven dat het Ministerie van Defensie over de meest geavanceerde beveiligingstechnieken beschikt, die in overeenstemming zijn met het DBB.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
7.	Vooralsnog blijkt niet dat Defensie reeds heeft vastgesteld welke personen toegang kunnen krijgen tot de standalone laptop en de eventuele persoonsgegevens die daarop verwerkt zijn.	<ul style="list-style-type: none"> - Het opstellen van een autorisatiematrix waaruit blijkt welke personen voor welke termijn toegang hebben tot de standalone laptop. - Daarnaast dient zorg te worden gedragen voor een regelmatige update van het gehanteerde wachtwoord en eventueel zorg te worden gedragen voor tweefactor authenticatie, voor zover dit nog niet uit het DBB volgt.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Deze beoogde activiteit is nog niet opgenomen in het verwerkingsregister van Defensie.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
8.	De verwerking van persoonsgegevens bij deze activiteit is vooralsnog niet opgenomen in het verwerkingsregister van Defensie.	De verwerking van persoonsgegevens bij deze activiteit opnemen in het verwerkingsregister.

Conclusie

CZSK heeft de wens om een GMI te ontwikkelen, waarmee interne en externe risico's kunnen worden gesignaleerd. Hoewel het GMI niet is gericht op het verwerken van persoonsgegevens, kunnen persoonsgegevens wel als bijvangst worden verwerkt. Op het moment dat een signaal, dat afkomstig is van de mobiele telefoon van een marinier, wordt gesignaleerd, kan uit het signaal mogelijk worden afgeleid wie de gebruiker is van het apparaat. CZSK beschikt op basis van de huidige wet- en regelgeving (nog) niet over een grondslag om bij de beoogde activiteit persoonsgegevens te mogen verwerken. Daarnaast wordt ook aan de overige beginselen uit artikel 5 AVG nog niet (volledig) voldaan. Alvorens een GMI daadwerkelijk kan worden gebruikt, is het noodzakelijk dat CZSK onder meer aandacht besteedt aan de informatieplicht, protocollen om minimale gegevens te verwerken, bewaartermijnen en het beveiligingsbeleid.

Activiteit 9B

Omschrijving activiteit 9B

Deze activiteit vond tijdens het onderzoek niet plaats.

Het Korps Mariniers van het Commando Zeestrijdkrachten (hierna: CZSK) heeft de wens om gebruik te maken van een geïntegreerd mobiel interceptieplatform (hierna: GMI). Het GMI verzamelt en verwerkt data door middel van Cyber and Electromagnetic Activities (hierna: CEMA). Hiermee kunnen onder andere radio-, wifi- en Bluetoothsignalen worden verwerkt. Het doel hiervan is de Operational Security (hierna: OPSEC) en de Digital Force Protection zeker te stellen en om de eigen defensiemedewerkers bewust te maken van de risico's en consequenties van de verspreiding van informatie.⁹⁸ Met een GMI kunnen kort gezegd interne en externe risico's in kaart worden gebracht.

Onder interne risico's worden signalen verstaan die afkomstig zijn van mobiele apparaten van de eigen mariniers en die getraceerd kunnen worden door een mogelijke vijand. Inzet van een GMI zorgt ervoor dat duidelijk in kaart wordt gebracht of er interne signalen worden uitgezonden. Ook kan worden bekeken van wie die interne signalen afkomstig zijn. Als een dergelijke signalering risico's voor de veiligheid van de betreffende eenheid met zich meebrengt kan CZSK, op basis van die signalering, maatregelen treffen om deze risico's te mitigeren.

Onder externe risico's worden signalen verstaan die afkomstig zijn van mobiele apparaten die zich buiten, maar in de nabijheid van, de betreffende eenheid bevinden. Inzet van een GMI zorgt ervoor dat in kaart wordt gebracht welke signalen er worden uitgezonden, waar die signalen van afkomstig zijn en of wel of geen potentieel risico bestaat voor de veiligheid van de betreffende eenheid. Op basis van die signalering kan CZSK maatregelen treffen om de risico's te mitigeren.

Met het gebruik van een GMI kunnen persoonsgegevens worden verwerkt van de eigen mariniers en van derden die niet aan Defensie zijn gelieerd en zich binn en het ontvangstbereik van het GMI bevinden. Om onderscheid aan te brengen in de verwerking van de persoonsgegevens van deze twee groepen en ter bevordering van de leesbaarheid van dit document, worden de mariniers hierna aangeduid als 'internen' en de derden die niet gerelateerd zijn aan Defensie als 'externen'.

⁹⁸ Onder te verzamelen en verwerken data wordt data verstaan die afkomstig is van de signalen die worden uitgezonden door de mobiele apparaten die de mariniers enerzijds en externen anderzijds bij zich dragen.

In deze uitwerking van activiteit 10B gaan wij in op de verwerking van persoonsgegevens van externen. In de uitwerking van activiteit 9A gaan wij in op de verwerking van persoonsgegevens van internen.

Gebruik geïntegreerd mobiel interceptieplatform (afgekort: GMI)	
Wie?	Commando Zeestrijdkrachten onder verantwoordelijkheid van de Minister van Defensie.
Wat?	Constateren signalen (telefoon, radio, etc.) in de kijkomgeving en het uitlezen van die signalen, waarbij mogelijk persoonsgegevens worden verwerkt.
Waar?	Wereldwijd. De scope van dit onderzoek beperkt zich tot gebruik op Nederlands grondgebied en op schepen en luchtvaartuigen die zich in Nederlandse wateren, respectievelijk het Nederlandse luchtruim, bevinden.
Wanneer?	Tijdens algemene gereedstelling (er is dan geen sprake van een regeringsbesluit/mandaat).
Waarom?	Door de omgeving in kaart te brengen kan de eenheid beter beschermd worden.
Hoe?	Opvangen signalen door middel van een antenne, het omzetten van de opgevangen signalen in een voor mensen leesbare vorm op de standalone laptop, het raadplegen van de gegevens die uit de signalen kunnen worden afgeleid.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van het CZSK zoals deze uit verschillende wet- en regelgeving blijken.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. CZSK is een krijgsmachtonderdeel binnen Defensie.

Algemeen organisatiebesluit Defensie 2021

Artikel 12 van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) geeft de volgende taak aan de Commandant Zeestrijdkrachten:

“De Commandant Zeestrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Zeestrijdkrachten;*
- b. De gereedstelling en instandhouding van de zeestrijdkrachten;*
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. Het binnen de gestelde normen en kader uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Zeestrijdkrachten;*
- e. Het beheer van de Kustwacht Nederland en de Kustwacht Caribische Gebied;*
- f. De advisering op het gebied van militair maritiem optreden.”*

Het beoogde gebruik van het GMI vindt plaats om digitale verkenningen te kunnen uitvoeren om de veiligheid van de mariniers te kunnen waarborgen. Door eventuele risico's – zoals afwijkende signalen – door middel van Cyber and Electromagnetic Activities (hierna: CEMA) vroegtijdig in kaart te brengen, kan CZSK tijdig daarop anticiperen. Het uitvoeren van digitale verkenningen kan – met een ruime interpretatie – als middel worden gezien om de zeestrijdkrachten in stand te houden, zoals genoemd in artikel 12, aanhef en onder b, AOD.

199

Subtaakbesluit Commando Zeestrijdkrachten 2010

Artikel 26 AOD bepaalt dat er subtaakbesluiten kunnen worden vastgesteld. CZSK beschikt over het Subtaakbesluit Commando Zeestrijdkrachten 2010 (hierna: subtaakbesluit). Dit subtaakbesluit voorziet de verschillende onderdelen binnen CZSK van een nadere taakomschrijving. Artikel 5 van het subtaakbesluit geeft de volgende taak aan de Directie Operaties:

“De directie Operaties staat onder leiding van de directeur Operaties die is belast met:

- a. het met inachtneming van de opdracht, planningskaders en (functionele) richtlijnen van de Commandant Zeestrijdkrachten geven van leiding aan de directie Operaties;*
- b. het ontwikkelen en onderhouden van maritiem-expeditionair vermogen in al zijn facetten;*
- c. het ontwikkelen en onderhouden van maritieme doctrines en tactieken;*
- d. het aanbrengen en behouden van de geoefendheid van enkelvoudige eenheden, samengestelde eenheden en een 'deployable' staf;*

- e. mede gelet op de taken van het Defensie Operatie Centrum, het, al dan niet als formerend Operationeel Commando, in opdracht en onder verantwoordelijkheid van de Commandant der Strijdkrachten uitvoeren van coördinerende activiteiten t.b.v. operaties;
- f. het coördineren van de ondersteuning van eenheden die worden ingezet door de Commandant der Strijdkrachten, dan wel de Belgische Chief of Defense voor zover die inzet in binationaal verband en via de organisatie van de Admiraal Benelux wordt aangestuurd;
- g. de operationele planning van operaties voorafgaande aan maar ook tijdens en na de operaties ten behoeve van het Defensie Operatie Centrum en het Belgische Center of Operations;
- h. het geven van leiding aan de Dienst der Hydrografie en in dat kader uitvoeren van hydrografische, oceanografische en meteorologische ondersteuning bij militair optreden met daarnaast systematisch zeebodemonderzoek en nautische kartering overeenkomstig internationale verdragen;
- i. het ontwikkelen en onderhouden van functionele richtlijnen – ten aanzien van het eigen terrein van verantwoordelijkheid – voor de gehele CZSK-organisatie;
- j. het binnen het Commando Zeestrijdkrachten optreden als aanspreekpunt voor de directeur van de directie Operaties van de Defensiestaf;
- k. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;
- l. de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de directie Operaties."

Het beoogde gebruik van het GMI kan mogelijk worden geschaard onder de uitvoering van een van de taken uit artikel 12 sub b AOD of artikel 5, sub b en c van het subtaakbesluit.

Toepassingsbereik AVG

Vaststellen scope activiteit in het kader van het onderzoek

Tijdens het interview is naar voren gekomen dat de inzet van een GMI onder uiteenlopende omstandigheden en op diverse locaties mogelijk moet zijn. Dit zorgt ervoor dat het Korps Mariniers, bij de inzet van een GMI, ook te maken kan krijgen met internationale en buitenlandse wet- en regelgeving voor de verwerking van (persoons)gegevens. In dit AVG-onderzoek beperken wij ons tot de inzet van een GMI op Nederlands grondgebied en op schepen en luchtvaartuigen die zich in Nederlandse wateren, respectievelijk het Nederlandse luchtruim, bevinden.

Onderhavig onderzoek richt zich op informatie gestuurd optreden door eenheden van het Ministerie van Defensie ten tijde van algemene gereedstelling. Omdat aan specifieke gereedstelling en aan inzet een regeringsbesluit of een besluit van de Minister van Defensie ten grondslag ligt, waaruit specifieke bevoegdheden voor de eenheden kunnen voortvloeien, wordt informatie gestuurd optreden ten tijde van specifieke gereedstelling en inzet buiten beoordeling gelaten in dit onderzoek.

Materieel toepassingsbereik

Respondent heeft aangegeven dat het GMI verscheidene signalen kan opvangen en verwerken, waaronder telefoonsignalen, radiosignalen, wifisignalen en Bluetoothsignalen. Wanneer de antenne van het GMI een signaal opvangt, wordt dit signaal verwerkt op zo'n manier dat het voor mensen begrijpelijk en leesbaar is. Deze begrijpelijke en leesbare versie van het signaal kan vervolgens worden afgelezen van de laptop die met het GMI verbonden is.

Op basis van een ontvangen telefoonsignaal kan mogelijk worden afgeleid wie de eigenaar en/of gebruiker van het toestel is en wat hij of zij ermee heeft gedaan. Het opgevangen signaal kan namelijk een hoop metadata prijsgeven, welke data herleidbaar kan zijn tot een individu. Het kan dan bijvoorbeeld gaan om de unieke MAC-adressen en locatiegegevens die kunnen worden gecombineerd met tijdstip en plaats, en mogelijke wifi- en Bluetooth namen van persoonlijke hardware. Wanneer een GMI wordt gebruikt kunnen er, afhankelijk van in hoeverre de signalen worden uitgelezen, persoonsgegevens worden verwerkt.

Voor gebruik van een GMI ten tijde van specifieke gereedstelling en inzet kan op grond van de Regeling gegevensbescherming militaire operaties (hierna: RGMO) (gedeeltelijk) worden afgeweken van de AVG. Dit gebeurt door middel van een regeringsbesluit dat, voorafgaand aan de specifieke gereedstelling of inzet, wordt opgesteld door de Minister van Defensie. Ten tijde van algemene gereedstelling, waarbij de krijgsmacht zich onder meer bezighoudt met algemene trainingsdoeleinden, is er geen sprake van een regeringsbesluit waarin gedeeltelijk kan worden afgeweken van de AVG. De AVG en de UAVG zijn dus onverkort van toepassing op het gebruik van een GMI ten tijde van algemene gereedstelling.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

Een GMI kan ook worden gebruikt buiten Nederland en buiten de Europese Economische Ruimte (hierna: 'EER'). Zelfs wanneer met het GMI persoonsgegevens worden verwerkt bijvoorbeeld op een marineschip dat zich in internationale wateren bevindt, is de AVG op deze verwerking van persoonsgegevens van toepassing. Zoals ook hierboven in de scopebepaling voor deze activiteit is toegelicht, beperken wij ons tot de inzet van een GMI op Nederlands grondgebied en op schepen die zich in Nederlandse wateren bevinden.

De AVG is dus van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

Voor de juridische beoordeling van de rechtmatigheid van de gegevensverwerking bij deze activiteit kan aansluiting worden gezocht bij de beoordeling van de rechtmatigheid bij activiteit 9A. Voor de uitwerking van de beoordeling over de rechtmatigheid verwijzen wij daarom naar de uitwerking bij activiteit 9A.

Concluderend merken wij op dat CZSK niet over een grondslag beschikt voor het verwerken van persoonsgegevens bij deze beoogde activiteit.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Het ontbreken van een wettelijke grondslag voor het gebruik van een GMI.	Het creëren van een formeel wettelijke grondslag, waaruit duidelijk kan worden afgeleid dat er een noodzaak bestaat om persoonsgegevens te verwerken. De verwerking van persoonsgegevens (ook als bijvangst) dient namelijk voorzienbaar te zijn bij wet. Een generieke taakomschrijving, waaruit bijvoorbeeld blijkt dat de Commandant der Zeestrijdkrachten

		zorg dient te dragen voor het waarborgen van de veiligheid van de mariniers, is in dit licht onvoldoende.
--	--	---

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

Respondent heeft aangegeven dat externen, wiens signalen door het GMI kunnen worden opgevangen, niet op de hoogte zijn van het feit dat hun signalen worden opgevangen en mogelijk ook worden uitgelezen.

Uitzonderingen op de informatieplicht

Artikel 13, 14 en 23 AVG en artikel 41 UAVG kennen enkele uitzonderingen op de informatieplicht in het kader van behoorlijkheid en transparantie.

203

De uitzondering in artikel 13 ziet op de situatie waarin persoonsgegevens rechtstreeks van betrokkene worden verzameld en betrokkene reeds over de informatie zoals genoemd in artikel 13 AVG beschikt. Bij het verzamelen van eventuele persoonsgegevens door middel van het GMI wordt de informatie ook rechtstreeks van betrokkene verkregen.⁹⁹ Betrokkenen zullen niet op de hoogte zijn van het feit dat signalen kunnen worden verwerkt. Daarnaast beschikken betrokkenen ook niet over alle te verstrekken informatie zoals genoemd in artikel 13 AVG. Dit is vanuit de context voor het beoogde gebruik van het GMI ook niet wenselijk. Echter daarom is de uitzondering op de informatieplicht in artikel 13 AVG op deze activiteit niet van toepassing.

De uitzonderingen in artikel 14 AVG zien op de situatie waarin persoonsgegevens niet rechtstreeks zijn verkregen van de betrokkene. Bij het verzamelen van eventuele persoonsgegevens door middel van het GMI wordt informatie juist wel direct van betrokkenen verkregen. De uitzonderingen op de informatieplicht in artikel 14 AVG zijn daarom niet van toepassing.

Op grond van artikel 23 AVG en het overeenkomstige artikel 41 UAVG kan een uitzondering worden gemaakt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de

⁹⁹ Vergelijk Richtsnoeren inzake transparantie overeenkomstig Verordening (EU)2016/679 van WG29, p. 16, paragraaf 26.

verwerker van toepassing zijn, op voorwaarde dat die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel is ter waarborging van:

- a) de nationale veiligheid
- b) landsverdediging
- c) de openbare veiligheid

Respondent gaf aan dat met het beoogde gebruik van het GMI de veiligheid van de mariniers of opvarenden kan worden gewaarborgd. Alhoewel kan worden gesteld dat dit doel indirect een bijdrage zou kunnen leveren aan de waarborging van de nationale veiligheid, landsverdediging en de openbare veiligheid, zijn wij van oordeel dat deze activiteit geen noodzakelijke en evenredige maatregel is ter waarborging van deze belangen. Bovendien zijn ons geen uitzonderingen in Unierechtelijk recht of lidstaatrechtelijk recht gebleken op grond waarvan CZSK bij de verwerking van persoonsgegevens bij deze activiteit een uitzondering kan maken op de informatieplicht.

Concluderend merken wij op dat aan het beginsel van behoorlijkheid en transparantie niet wordt voldaan.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
2.	De juridische mogelijkheid bestaat om Defensie te ontslaan van haar verplichting om betrokkenen van informatie te voorzien, mits die uitzondering voortvloeit uit een Unierechtelijke of lidstaatrechtelijke bepaling.	Wetgeving ontwerpen op basis waarvan gebruik van een GMI toegestaan is en betrokkenen daarover niet hoeven te worden geïnformeerd.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

Respondent heeft aangegeven dat verdachte externe signalen vroegtijdig gesignaleerd dienen te worden, om de veiligheid van de eenheid te kunnen waarborgen. Ter illustratie gaf respondent aan dat een buitenlands telefoonsignaal tijdens een trainingsmissie verdacht kan zijn. Hetzelfde geldt

voor een wifi-netwerk, bijvoorbeeld van de McDonalds, dat midden op zee wordt aangeboden.

Respondent gaf aan dat de wens bestaat om informatie (en daarbij eventuele persoonsgegevens) die wordt verkregen door gebruik van het GMI, onder omstandigheden ook te koppelen aan informatie afkomstig uit andere bronnen. Hierbij bestaat het risico dat bij de koppeling van (persoons)gegevens wordt afgeweken van het oorspronkelijke doel waarvoor de (persoons)gegevens in beginsel zijn verzameld.

Het beginsel van doelbinding lijkt bij deze beoogde activiteit vooralsnog te worden nageleefd.

Mogelijke knelpunten		Aanbevelingen
Juridisch		
3.	Het risico bestaat dat bij koppeling van data wordt afgeweken van het oorspronkelijke doel waarvoor persoonsgegevens in beginsel zijn verzameld.	In het kader van doelbinding is het van belang om vooraf vast te leggen onder welke omstandigheden informatie die is verkregen met het GMI kan worden gekoppeld aan informatie uit andere bronnen. In ogenschouw dient te worden genomen dat de koppeling plaatsvindt in overeenstemming met het oorspronkelijke doel waarvoor de gegevens in beginsel zijn verzameld.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Respondent heeft aangegeven dat de wens bestaat om het GMI te allen tijde ingeschakeld te hebben, om zo signalen te kunnen opvangen die zich in de omgeving bevinden. Met het GMI kunnen dan op basis van Electronic Support Measures (ESM) signalen worden opgepikt en geanalyseerd, om eventuele bedreigingen te herkennen. Op deze wijze wordt een bepaald 'normbeeld' gecreëerd, zodat eventueel daarvan afwijkende signalen kunnen worden geanalyseerd en al dan niet als bedreiging kunnen worden aangemerkt. Daar kan vervolgens op geanticipeerd worden. Het creëren van een normbeeld en het constateren van eventuele afwijkingen of potentiële bedreigingen is alleen mogelijk wanneer het GMI over een bepaalde periode voor langere tijd wordt

ingeschakeld. Hieraan is inherent dat ook persoonsgegevens worden verwerkt. Dit staat op gespannen voet met het beginsel van minimale gegevensverwerking.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
4.	Voor het vaststellen van een normbeeld dient het GMI gedurende langere tijd te worden ingezet, waarbij het inherent is dat daarbij persoonsgegevens als bijvangst zullen worden verwerkt.	<p>In het kader van minimale gegevensverwerking verdient het aanbeveling om een protocol op te stellen waarin is vastgesteld wanneer een signaal als ongewenst of verdacht wordt aangemerkt en onder welke omstandigheden diepgaander onderzoek is toegestaan. Het verdient daarnaast aanbeveling om goed te documenteren indien en waarom naar de volgende stap wordt overgegaan. Het normbeeld wordt dan niet automatisch vastgelegd door ongericht alle signalen op te vangen en uit te lezen, maar geschiedt weloverwogen en zorgvuldig door het stap voor stap te benaderen en te documenteren.</p> <p>Ter illustratie: wanneer er een Afghaans telefoonsignaal wordt gesignaleerd tijdens een trainingsmissie in Nederland, zou dat als verdacht kunnen worden aangemerkt. Dit kan weer anders zijn wanneer de trainingsmissie wordt belegd naast een asielzoekerscentrum. Het verdient aanbeveling om alleen dan het signaal verder uit te lezen en daarbij eventueel persoonsgegevens te verwerken wanneer de aanwezigheid van het signaal niet kan worden verklaard.</p>

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Voor de juridische beoordeling van de juistheid van de gegevens van externen kan aansluiting worden gezocht bij de juridische beoordeling van de juistheid van de gegevens van internen bij activiteit 9A.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren valt, dan moeten de persoonsgegevens worden gewist.

Voor de juridische beoordeling van de opslagbeperking van de gegevens van externen kan aansluiting worden gezocht bij de juridische beoordeling van de juistheid van de gegevens van internen bij activiteit 9A.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
5.	Vooralsnog ontbreken specifieke bewaartermijnen voor eventuele persoonsgegevens die bij het gebruik van een GMI worden verwerkt.	<ul style="list-style-type: none">- Generieke bewaartermijnen vastleggen en een protocol opstellen waaruit blijkt op welke manier de vernietiging van de persoonsgegevens plaatsvindt. Ter illustratie: voor signalen die worden opgevangen door een GMI tijdens een trainingsmissie kan een bewaartermijn gehanteerd worden tot zes maanden na afloop van de trainingsmissie.- Indien het noodzakelijk is om persoonsgegevens langer te bewaren, dienen er aanknopingspunten te worden vastgelegd in het protocol onder welke omstandigheden langer bewaren geoorloofd is.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Voor de juridische beoordeling van de integriteit en vertrouwelijkheid van de gegevens van externen kan aansluiting worden gezocht bij de juridische beoordeling van de integriteit en vertrouwelijkheid van internen bij activiteit 9A.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
6.	Vooralsnog blijkt niet dat Defensie reeds heeft vastgesteld welke personen toegang kunnen krijgen tot de standalone laptop en de eventuele persoonsgegevens die daarop verwerkt zijn.	<ul style="list-style-type: none">- Het opstellen van een autorisatiematrix waaruit blijkt welke personen voor welke termijn toegang hebben tot de standalone laptop.- Daarnaast dient zorg te worden gedragen voor een regelmatige update van het gehanteerde wachtwoord en eventueel zorg te worden gedragen voor tweefactor authenticatie, voor zover dit nog niet uit het DBB volgt.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Deze beoogde activiteit is nog niet opgenomen in het verwerkingsregister van Defensie.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
7.	De verwerking van persoonsgegevens bij deze activiteit is vooralsnog niet opgenomen in het verwerkingsregister van Defensie.	De verwerking van persoonsgegevens bij deze activiteit opnemen in het verwerkingsregister.

Conclusie

CZSK heeft de wens om een GMI te ontwikkelen, waarmee interne en externe risico's kunnen worden gesignaleerd. Hoewel het GMI niet is gericht op het verwerken van persoonsgegevens, kunnen persoonsgegevens wel als bijvangst worden verwerkt. Op het moment dat bij het beoogde gebruik van een GMI door middel van CEMA signalen worden verwerkt, worde daarbij mogelijk persoonsgegevens als bijvangst verwerkt. CZSK beschikt op basis van de huidige wet- en regelgeving (nog) niet over een grondslag om bij de beoogde activiteit persoonsgegevens te mogen verwerken. Daarnaast wordt ook aan de overige beginselen uit artikel 5 AVG nog niet (volledig) voldaan. Alvorens een GMI daadwerkelijk kan worden gebruikt, is het noodzakelijk dat CZSK onder meer aandacht besteedt aan de informatieplicht, protocollen om minimale gegevens te verwerken, bewaartermijnen en het beveiligingsbeleid.

Activiteit 10A

Omschrijving activiteit 10A

CZSK voert digitale verkenningen uit ten behoeve van eigen operationele informatie, waarbij aan de hand van Defensie-gerelateerde zoektermen en hashtags op het internet wordt gezocht naar (operationele) informatie die (mogelijk) ongewenst gedeeld is.

Door voorafgaand aan en tijdens een trainingsmissie te onderzoeken of er informatie over de trainingsmissie ongewenst openbaar is gemaakt, kan CZSK tijdig maatregelen treffen om de veiligheid van de mariniers te blijven waarborgen. Een marinier die bijvoorbeeld een foto van het dagprogramma op Twitter heeft gedeeld kan dan worden aangesproken op zijn gedrag. Wanneer wordt geconstateerd dat een lokale journalist operationele informatie, zoals procedures, heeft verwerkt in zijn krantenartikel, dan probeert CZSK deze informatie te (laten) verwijderen.

Voorbeeld: jaarlijks trekken verschillende marinierseenheden naar Noorwegen voor een Joint Arctic Training (hierna: JAT). Daar leren zij omgaan met erbarmelijke weersomstandigheden. Het Ministerie van Defensie (hierna: Defensie) deelt op haar YouTube-kanaal regelmatig beeldmateriaal van zulke trainingsmissies en publiceert blogs over de ervaringen van de mariniers op haar website. De exacte locatie van de mariniers wordt echter niet met de buitenwereld gedeeld. Ook operationele informatie blijft verborgen. De veiligheid van de mariniers kan namelijk in het gedrang komen op het moment dat vijandige buitenstaanders dergelijke kennis verkrijgen. Om zulke kennisuitwisseling te voorkomen voert CZSK digitale verkenningen uit, waarbij aan de hand van Defensie-gerelateerde zoektermen en hashtags op het internet wordt gezocht naar informatie die (mogelijk) ongewenst gedeeld is en bijvoorbeeld terug te vinden is in sociale mediaberichten van mariniers of publicaties van Noorse kranten.

210

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van CZSK, zoals deze uit verschillende wet- en regelgeving blijken.

Algemeen organisatiebesluit Defensie 2021

Artikel 12 van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) geeft de volgende taak aan de Commandant Zeestrijdkrachten:

“De Commandant Zeestrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Zeestrijdkrachten;*

- b. De gereedstelling en instandhouding van de zeestrijdkrachten;
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;
- d. Het binnen de gestelde normen en kader uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Zeestrijdkrachten;
- e. Het beheer van de Kustwacht Nederland en de Kustwacht Caribische Gebied;
- f. De advisering op het gebied van militair maritiem optreden."

Subtaakbesluit Commando Zeestrijdkrachten 2010

Artikel 26 AOD bepaalt dat er subtaakbesluiten kunnen worden vastgesteld. CZSK beschikt over het Subtaakbesluit Commando Zeestrijdkrachten 2010 (hierna: subtaakbesluit). Dit subtaakbesluit voorziet de verschillende onderdelen binnen CZSK van een nadere taakomschrijving. Artikel 5 van het subtaakbesluit geeft de volgende taak aan de directie Operaties:

"De directie Operaties staat onder leiding van de directeur Operaties die is belast met:

- a. *het met inachtneming van de opdracht, planningskaders en (functionele) richtlijnen van de Commandant Zeestrijdkrachten geven van leiding aan de directie Operaties;*
- b. *het ontwikkelen en onderhouden van maritiem-expeditionair vermogen in al zijn facetten;*
- c. *het ontwikkelen en onderhouden van maritieme doctrines en tactieken;*
- d. *het aanbrengen en behouden van de geoefendheid van enkelvoudige eenheden, samengestelde eenheden en een 'deployable' staf;*
- e. *mede gelet op de taken van het Defensie Operatie Centrum, het, al dan niet als formerend Operationeel Commando, in opdracht en onder verantwoordelijkheid van de Commandant der Strijdkrachten uitvoeren van coördinerende activiteiten t.b.v. operaties;*
- f. *het coördineren van de ondersteuning van eenheden die worden ingezet door de Commandant der Strijdkrachten, dan wel de Belgische Chief of Defense voor zover die inzet in binationaal verband en via de organisatie van de Admiraal Benelux wordt aangestuurd;*
- g. *de operationele planning van operaties voorafgaande aan maar ook tijdens en na de operaties ten behoeve van het Defensie Operatie Centrum en het Belgische Center of Operations;*
- h. *het geven van leiding aan de Dienst der Hydrografie en in dat kader uitvoeren van hydrografische, oceanografische en meteorologische ondersteuning bij militair optreden met daarnaast systematisch*

zeebodemonderzoek en nautische kartering overeenkomstig internationale verdragen;

- i. het ontwikkelen en onderhouden van functionele richtlijnen – ten aanzien van het eigen terrein van verantwoordelijkheid – voor de gehele CZSK-organisatie;*
- j. het binnen het Commando Zeestrijdkrachten optreden als aanspreekpunt voor de directeur van de directie Operaties van de Defensiestaf;*
- k. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;*
- l. de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de directie Operaties."*

Het uitvoeren van digitale verkenningen kan ons inziens als middel worden gezien voor het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, zoals genoemd onder artikel 5 sub k van het subtaakbesluit.

Toepassingsbereik AVG

212

Materieel toepassingsbereik

Hoewel de digitale verkenningen niet zijn gericht op het verkrijgen van persoonsgegevens, is het enkele raadplegen van persoonsgegevens uit kranten, sociale mediaberichten en andere bronnen al een vorm van geheel of gedeeltelijke geautomatiseerde verwerking van die persoonsgegevens.¹⁰⁰

De verwerking van persoonsgegevens in deze activiteit gebeurt weliswaar door de krijgsmacht, maar niet in het kader van de operationele inzet van die krijgsmacht. Dit brengt met zich mee dat van de uitzonderingssituaties uit artikel 2, tweede lid, AVG, geen sprake is. De AVG is daardoor van toepassing op de verwerking van persoonsgegevens in deze activiteit.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

De AVG is dus wel van toepassing op deze activiteit.

¹⁰⁰ Er is ook sprake van verwerking van persoonsgegevens, wanneer men niet de intentie heeft om die persoonsgegevens te verwerken. Wanneer persoonsgegevens worden verwerkt met als doel het verkrijgen van inzicht, is de AVG van toepassing. Vgl. 'Onderzoek naleving Algemene verordening gegevensbescherming Experimenteertomgeving Land Information Manoeuvre Centre (LIMC)' d.d. 31 maart 2021.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens verwerkt mogen worden als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd waarbij het voor de betrokkene duidelijk moet zijn dat er persoonsgegevens worden verwerkt. Bovendien is het enkel toegestaan om persoonsgegevens op basis van deze grondslag te verwerken als het noodzakelijk is voor de vervulling van de publieke taak.

Uit overweging 45 van de AVG volgt dat de verwerking voor een succesvol beroep op artikel 6 lid 1 sub c AVG of artikel 6 lid 1 sub e AVG een grondslag moet hebben in een Unierechtelijke of lidstaatrechtelijke bepaling. Overweging 41 van de AVG voegt daaraan toe dat de rechtsgrond of wetgevingsmaatregel evenwel duidelijk en nauwkeurig moet zijn, en de toepassing daarvan voorspelbaar moet zijn voor degenen op wie deze van toepassing is.

213

Daarnaast bepaalt artikel 10 Gw dat een overheidsinstantie zich in beginsel niet mag inmengen in de persoonlijke levenssfeer van een burger, tenzij een wet in formele zin hiervoor een grondslag biedt én die wet regels stelt voor het beschermen van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens.

Dit brengt met zich mee dat de taak van algemeen belang ook moet voortvloeien uit een Unierechtelijke of lidstaatrechtelijke bepaling. Onder het kopje 'taakomschrijving' hebben wij opgemerkt dat deze activiteit volgens ons mogelijk geschaard kan worden onder de taak uit artikel 5 sub k van het subtaakbesluit. Wij zijn echter van mening dat het subtaakbesluit niet als grondslag kan dienen voor de verwerking van persoonsgegevens bij deze activiteit, omdat het subtaakbesluit niet kan worden aangemerkt als lidstaatrechtelijke bepaling met formele rechtskracht.

Wij zijn dan ook van mening dat een beroep op het algemeen belang geen kans van slagen heeft.

Gerechtvaardigd belang

Artikel 6 lid 1 sub f AVG bepaalt dat de verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De laatste volzin van artikel 6 lid 1 sub f AVG voegt daaraan toe dat overheidsinstanties in het kader van de uitoefening van hun taken geen beroep kunnen doen op artikel 6 lid 1 sub f AVG.

In hoofdstuk 5 van dit rapport hebben wij uiteengezet dat een beroep op het gerechtvaardigd belang door overheidsinstanties alleen mogelijk is voor typisch bedrijfsmatige handelingen van die overheidsinstanties. Activiteiten zoals de onderhavige activiteit, die toezien op of samenhangen met gereedstellen/inzet van de krijgsmacht zijn ons inziens in geen zin aan te merken als een typisch bedrijfsmatige handeling. Gelet op het bovenstaande kan CZSK bij deze activiteit geen beroep doen op verwerking van persoonsgegevens op grond van een gerechtvaardigd belang uit artikel 6 lid 1 sub f AVG.

214

Concluderend merken wij op dat CZSK niet over een grondslag beschikt voor het verwerken van persoonsgegevens bij deze activiteit.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	De bevoegdheid voor het verwerken van persoonsgegevens kan niet worden ontleend uit een wet in formele zin.	Het vaststellen van een wet in formele zin waaruit de bevoegdheid voor het verwerken van persoonsgegevens kan worden ontleend.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

Artikel 14 lid 3 sub b AVG bepaalt dat betrokkene op het moment van het eerste contact op de hoogte moet worden gebracht van de verwerking van zijn persoonsgegevens en de verdere informatie uit artikel 14 lid 1 jº lid 2 AVG. De mariniers, wiens persoonsgegevens bij de digitale verkenningen kunnen worden verwerkt, worden voorafgaand aan de digitale verkenningen geïnformeerd over het doel van de verkenningen, de manier waarop de verkenningen worden uitgevoerd en de persoonsgegevens die bij de verkenningen eventueel verwerkt kunnen worden. Respondent heeft aangegeven dat de mariniers tijdens hun opleiding ook worden geïnformeerd over het belang van het afschermen van sociale mediaprofielen.

Wij zijn van mening dat mariniers voorafgaand aan de digitale verkenningen al worden geïnformeerd over de identiteit van de verwerkingsverantwoordelijke (1a), de verwerkingsdoeleinden (1c), de betrokken categorieën van persoonsgegevens (1d), de ontvangers van de persoonsgegevens (1e) en de bron van de persoonsgegevens (2f).¹⁰¹ Wanneer CZSK constateert dat een marinier operationele informatie heeft gedeeld via sociale media, leidt dit er in de praktijk toe dat de marinier op zijn gedrag wordt aangesproken. Wij zijn van mening dat de betreffende marinier dan nog gewezen moet worden op de overige informatie uit artikel 14 lid 2 AVG.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
2.	Artikel 14 AVG bepaalt dat de betrokkene ook informatie moet ontvangen over: de contactgegevens van de Functionaris voor Gegevensbescherming (1b), de bewaartermijn van de persoonsgegevens (2a), de rechten van betrokkene (2c) en het klachtrecht (2e).	<ul style="list-style-type: none"> - Het opnemen van een passage in de privacyverklaring voor medewerkers van Defensie, zodat de mariniers, voorafgaand aan de eventuele raadpleging van hun sociale mediaprofielen, op de hoogte zijn van de informatie uit artikel 14 AVG. - Een bepaling opnemen in de Militaire Ambtenarenwet 1931, waarin wordt bepaald dat mobiele apparaten en sociale mediaprofielen van medewerkers van Defensie kunnen worden gescreend.

¹⁰¹ De genoemde codering heeft betrekking op de leden en nummering van artikel 14 AVG.

Gelet hierop zijn wij van mening dat nog niet volledig aan het beginsel van behoorlijkheid en transparantie wordt voldaan.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

Het uitvoeren van digitale verkenningen en het eventuele raadplegen van daarbij voorkomende persoonsgegevens vindt plaats met als doel het (laten) verwijderen van ongewenst geleeke informatie, waarmee wordt voorkomen dat deze informatie verder wordt verspreid. Respondent heeft aangegeven dat de digitale verkenningen niet worden uitgevoerd met het oogmerk om de bron van de geleeke informatie te achterhalen.

Gelet hierop zijn wij van mening dat aan het beginsel van doelbinding wordt voldaan.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

216

Bij het uitvoeren van digitale verkenningen kunnen de volgende persoonsgegevens worden geraadpleegd: naam/gebruikersnaam van de sociale mediagebruiker, eventuele profielfoto van de sociale mediagebruiker (voor zover die foto herleidbaar is tot een persoon), namen van journalisten, eventuele persoonsgegevens die in of bij de operationele informatie te vinden is.

Respondent heeft aangegeven dat wanneer de geleeke informatie herleidbaar is tot een marinier, deze marinier op zijn of haar gedrag wordt aangesproken. Deze informatie wordt niet gekoppeld aan andere informatie uit bijvoorbeeld het personeelsdossier van de betreffende marinier. Nu er niet meer persoonsgegevens worden verwerkt dan noodzakelijk is voor het te bereiken doel, zijn wij van mening dat aan het beginsel van dataminimalisatie wordt voldaan.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verwerkingsverantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Respondent heeft aangegeven dat er bij digitale verkenningen sociale mediaprofielen van mariniers kunnen worden geraadpleegd, wanneer dat sociale mediaprofiel bij de zoekopdracht op Defensie-gerelateerde zoektermen en hashtags zichtbaar wordt. Voor zover die marinier operationele informatie heeft gedeeld, zal hij daarop worden aangesproken. Respondent heeft aangegeven dat de marinier alleen op zijn gedrag wordt aangesproken, wanneer vast staat dat hij het bericht heeft geplaatst. Er wordt dus niet zonder meer uitgegaan van de juistheid van de persoonsgegevens in het sociale mediaprofiel. CZSK verifieert eerst of het sociale mediaprofiel daadwerkelijk van de betreffende marinier is. Mocht er sprake zijn van het ernstig lekken van gerubriceerde informatie, dan zal er melding van worden gemaakt bij de MIVD en is het niet aan Defensie om hier verder actie op te ondernemen.

Daarnaast heeft respondent aangegeven dat er bij digitale verkenningen ook publicaties kunnen worden geraadpleegd, wanneer deze bij de zoekopdracht op Defensie-gerelateerde zoektermen en hashtags zichtbaar wordt. Indien er in die publicaties ook persoonsgegevens zijn verwerkt, dan mag verondersteld worden dat die gegevens met de nodige zorgvuldigheid openbaar zijn gemaakt en dus juist zijn.

Gelet hierop zijn wij van mening dat wordt voldaan aan het beginsel van juistheid.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalt, dan moeten de persoonsgegevens worden gewist.

De sociale mediaberichten die worden waargenomen tijdens een digitale verkenning worden uitsluitend geraadpleegd. Deze sociale mediaberichten worden niet opgeslagen. Mocht een marinier gehoor geven aan het verzoek om het sociale mediabericht te verwijderen, dan is hernieuwde raadpleging door CZSK ook niet meer mogelijk.

Respondent heeft de wens uitgesproken om mariniers bewust te maken van de risico's van sociale mediaberichten aan de hand van concrete voorbeelden.

Respondent wil daarvoor een database aanmaken met sociale mediaberichten die in het verleden zijn gepubliceerd. Respondent heeft aangegeven dat de sociale mediaberichten, met toestemming van de betreffende marinier, zullen worden gepseudonimiseerd. Onzes inziens hoeft CZSK daarvoor niet bestaande sociale mediaberichten te gebruiken. Er kan namelijk ook gebruik worden gemaakt van fictieve voorbeelden, waarbij er geen persoonsgegevens worden verwerkt. Deze fictieve voorbeelden kunnen wel op bestaande berichten zijn gebaseerd.

Wanneer CZSK operationele informatie aantreft in nieuwsberichten of publicaties, slaat CZSK deze nieuwsberichten op en probeert CZSK de daarin voorkomende informatie te verwijderen om (verdere) schade te voorkomen. Respondent heeft aangegeven dat er geen bewaartermijnen zijn vastgesteld.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
3.	CZSK heeft geen bewaartermijnen vastgesteld voor de publicaties die worden opgeslagen en waar eventueel persoonsgegevens in voorkomen.	Het vaststellen van bewaartermijnen en deze bewaartermijnen vastleggen in de selectielijst van Defensie.

218

Wij zijn van mening dat met het ontbreken van bewaartermijnen nog niet volledig aan het beginsel van opslagbeperking wordt voldaan.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Ongewenste sociale mediaberichten van mariniers zullen uitsluitend door CZSK worden geraadpleegd, teneinde die persoon erop te kunnen aanspreken om (verdere) schade door de gelekte informatie te voorkomen. Deze berichten worden niet opgeslagen en het aanspreken van de marinier is in beginsel zonder gevolgen, tenzij de marinier op ernstige wijze gerubriceerde informatie heeft gelekt. In dat geval wordt er melding gemaakt bij de MIVD. De MIVD schat dan het risico in en neemt eventueel op basis van de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: WIV 2017) maatregelen.

Wanneer de marinier door CZSK zelf op zijn gedrag wordt aangesproken, wordt het gedrag van de marinier niet gedeeld met andere mariniers of eenheden van Defensie.

Wij zijn van oordeel dat hiermee aan het beginsel van integriteit en vertrouwelijkheid wordt voldaan.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Over de verwerking van persoonsgegevens in deze activiteit is niets in het verwerkingenregister terug te vinden.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
4.	De verwerking van persoonsgegevens is niet terug te vinden in het verwerkingenregister.	Het opnemen van de activiteit in het verwerkingenregister.

219

Wij zijn van mening dat hiermee nog niet volledig aan de verantwoordingsplicht wordt voldaan.

Conclusie

CZSK raadpleegt sociale mediaberichten en daarbij behorende persoonsgegevens bij het uitvoeren van digitale verkenningen. Hoewel deze activiteit mogelijk geschaard kan worden onder de taak van de directie Operaties uit artikel 5 sub k van het subtaakbesluit, kan uit die taakomschrijving geen bevoegdheid worden ontleend in de zin van artikel 6 lid 1 sub e AVG. Ook een beroep op artikel 6 lid 1 sub f AVG heeft geen kans van slagen, waardoor de directie Operaties niet over een grondslag beschikt om bij deze activiteit persoonsgegevens te verwerken. Voor zover CZSK een grondslag weet te creëren om persoonsgegevens te verwerken, moet er nog aandacht worden besteed aan de informatieplicht, de bewaartermijnen en het verwerkingenregister om volledig aan de verplichtingen uit de AVG te voldoen.

Activiteit 10B

Omschrijving activiteit 10B

Het Commando Zeestrijdkrachten (hierna: CZSK) voert digitale verkenningen uit door openbare nieuwsbronnen te raadplegen. Aan de hand van de informatie uit deze nieuwsbronnen brengt CZSK in kaart wat er speelt in mogelijke conflictgebieden, zodat een eventuele missie met de nodige voorkennis wordt ingegaan.

Voorbeeld: overal op de wereld doen zich conflicten voor. Zo ook in Ethiopië, waar de situatie allesbehalve stabiel is. Om goed voorbereid te zijn op eventuele inzet, weet CZSK graag van tevoren wat er in welk conflictgebied speelt. Door openbare nieuwsbronnen te raadplegen brengt CZSK in kaart wat er in Ethiopië speelt.

Bij het in kaart brengen van een conflictgebied aan de hand van openbare nieuwsbronnen, kan het voorkomen dat er persoonsgegevens worden verwerkt. Hoewel deze persoonsgegevens in alle gevallen al openbaar zijn, is er ook bij het verzamelen van persoonsgegevens uit openbare nieuwsbronnen sprake van een verwerking van persoonsgegevens in de zin van de AVG. Wanneer de geldende wet- en regelgeving wordt gevolgd, is CZSK pas bevoegd om dergelijke persoonsgegevens te verwerken op het moment dat er een regeringsbesluit tot inzet is genomen en CZSK over het mandaat beschikt om dergelijke werkzaamheden uit te voeren. Respondent liet echter weten dat de voorbereidingstijd veel te kort is als vanaf het moment dat het regeringsbesluit is genomen pas wordt begonnen met het in kaart brengen van de omgeving. Respondent acht het daarom van belang om voortdurend mogelijke conflictgebieden te monitoren op aldaar aanwezige groeperingen en andere relevante veiligheidsrisico's, zoals de modus operandi, gebruikte wapens en locaties van incidenten. Er wordt niet specifiek gezocht op persoonsgegevens om bijvoorbeeld netwerken in kaart te brengen.

Door voortdurend conflictgebieden in de wereld te monitoren kan er snel geanticipeerd worden op het moment dat de regering besluit over te gaan tot inzet van de mariniers in dat conflictgebied. Het doel hierbij is om (in algemene zin) te weten wat er speelt in een bepaald conflictgebied. Tijdens het interview is naar voren gekomen dat mariniers binnen 48 uur klaar moeten staan om te worden ingezet.¹⁰² Om een goede voorbereiding te garanderen verzamelt CZSK, voorafgaand aan een regeringsbesluit tot inzet, alvast kranten, publicaties en

¹⁰² Volgens respondent vloeit dit voort uit de Aanwijzing Gereedstelling Defensie (AGDEF).

ontsloten informatie van ketenpartners.¹⁰³ Deze informatie wordt opgeslagen op de SharePoint en verwerkt in de briefing op het moment dat het regeringsbesluit is genomen.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van CZSK, zoals deze uit verschillende wet- en regelgeving blijken.

Algemeen organisatiebesluit Defensie 2021

Artikel 12 van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) geeft de volgende taak aan de Commandant Zeestrijdkrachten:

"De Commandant Zeestrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Zeestrijdkrachten;*
- b. De gereedstelling en instandhouding van de zeestrijdkrachten;*
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. Het binnen de gestelde normen en kader uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Zeestrijdkrachten;*
- e. Het beheer van de Kustwacht Nederland en de Kustwacht Caribische Gebied;*
- f. De advisering op het gebied van militair maritiem optreden."*

221

Subtaakbesluit Commando Zeestrijdkrachten 2010

Artikel 26 AOD bepaalt dat er subtaakbesluiten kunnen worden vastgesteld. CZSK beschikt over het Subtaakbesluit Commando Zeestrijdkrachten 2010 (hierna: subtaakbesluit). Dit subtaakbesluit voorziet de verschillende onderdelen binnen CZSK van een nadere taakomschrijving. Artikel 5 van het subtaakbesluit geeft de volgende taak aan de directie Operaties:

"De directie Operaties staat onder leiding van de directeur Operaties die is belast met:

- a. het met inachtneming van de opdracht, planningskaders en (functionele) richtlijnen van de Commandant Zeestrijdkrachten geven van leiding aan de directie Operaties;*

¹⁰³ Onder ontsloten informatie van ketenpartners wordt informatie verstaan die afkomstig is van buitenlandse krijgsmachten. Ter illustratie: de Franse krijgsmacht bevindt zich al in Ethiopië en verwerkt daar persoonsgegevens die afkomstig zijn uit openbare bronnen. Aangezien zij zich daar bevinden beschikken zij over een mandaat om dat te doen. Zij kunnen die informatie vervolgens ook delen met de Nederlandse krijgsmacht. In bepaalde gevallen worden ervaringen van die ketenpartners ook gedeeld.

- b. het ontwikkelen en onderhouden van maritiem-expeditionair vermogen in al zijn facetten;
- c. het ontwikkelen en onderhouden van maritieme doctrines en tactieken;
- d. het aanbrengen en behouden van de geoefendheid van enkelvoudige eenheden, samengestelde eenheden en een 'deployable' staf;
- e. mede gelet op de taken van het Defensie Operatie Centrum, het, al dan niet als formerend Operationeel Commando, in opdracht en onder verantwoordelijkheid van de Commandant der Strijdkrachten uitvoeren van coördinerende activiteiten t.b.v. operaties;
- f. het coördineren van de ondersteuning van eenheden die worden ingezet door de Commandant der Strijdkrachten, dan wel de Belgische Chief of Defense voor zover die inzet in binationaal verband en via de organisatie van de Admiraal Benelux wordt aangestuurd;
- g. de operationele planning van operaties voorafgaande aan maar ook tijdens en na de operaties ten behoeve van het Defensie Operatie Centrum en het Belgische Center of Operations;
- h. het geven van leiding aan de Dienst der Hydrografie en in dat kader uitvoeren van hydrografische, oceanografische en meteorologische ondersteuning bij militair optreden met daarnaast systematisch zeebodemonderzoek en nautische kartering overeenkomstig internationale verdragen;
- i. het ontwikkelen en onderhouden van functionele richtlijnen – ten aanzien van het eigen terrein van verantwoordelijkheid – voor de gehele CZSK-organisatie;
- j. het binnen het Commando Zeestrijdkrachten optreden als aanspreekpunt voor de directeur van de directie Operaties van de Defensiestaf;
- k. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;
- l. de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de directie Operaties."

Het raadplegen en opslaan van nieuwsberichten over conflictgebieden in de wereld kan ons inziens als middel worden gezien voor het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, zoals genoemd onder artikel 5 sub k van het subtaakbesluit.

Toepassingsbereik AVG

Materieel toepassingsbereik

Het raadplegen en opslaan op de SharePoint van nieuwsberichten en daarin voorkomende persoonsgegevens kwalificeert als een geheel of gedeeltelijke geautomatiseerde verwerking van die persoonsgegevens.

De verwerking van persoonsgegevens in deze activiteit gebeurt weliswaar door de krijgsmacht, maar niet in het kader van de operationele inzet van die krijgsmacht. Dit brengt met zich mee dat van de uitzonderingssituaties uit artikel 2, tweede lid, AVG, geen sprake is. De AVG is daardoor van toepassing op de verwerking van persoonsgegevens in deze activiteit.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

De AVG is dus wel van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. de rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

223

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens verwerkt mogen worden als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd waarbij het voor de betrokkene duidelijk moet zijn dat er persoonsgegevens worden verwerkt. Bovendien is het enkel toegestaan om persoonsgegevens op basis van deze grondslag te verwerken als het noodzakelijk is voor de vervulling van de publieke taak.

Uit overweging 45 van de AVG volgt dat de verwerking voor een succesvol beroep op artikel 6 lid 1 sub c AVG of artikel 6 lid 1 sub e AVG een grondslag moet hebben in een Unierechtelijke of lidstaatrechtelijke bepaling. Overweging 41 van de AVG voegt daaraan toe dat de rechtsgrond of wetgevingsmaatregel evenwel duidelijk en nauwkeurig moet zijn, en de toepassing daarvan voorspelbaar moet zijn voor degenen op wie deze van toepassing is.

Daarnaast bepaalt artikel 10 Gw dat een overheidsinstantie zich in beginsel niet mag inmengen in de persoonlijke levenssfeer van een burger, tenzij een wet in formele zin hiervoor een grondslag biedt én die wet regels stelt voor het

beschermen van de persoonlijke levenssfeer bij het verwerken van persoonsgegevens.

Dit brengt met zich mee dat de taak van algemeen belang ook moet voortvloeien uit een Unierechtelijke of lidstaatrechtelijke bepaling. Onder het kopje 'taakomschrijving' hebben wij opgemerkt dat deze activiteit volgens ons mogelijk geschaard kan worden onder de taak uit artikel 5 sub k van het subtaakbesluit. Wij zijn echter van mening dat het subtaakbesluit niet als grondslag kan dienen voor de verwerking van persoonsgegevens bij deze activiteit, omdat het subtaakbesluit niet kan worden aangemerkt als lidstaatrechtelijke bepaling met formele rechtskracht.

Wij zijn dan ook van mening dat een beroep op het algemeen belang geen kans van slagen heeft.

Gerechtvaardigd belang

Artikel 6 lid 1 sub f AVG bepaalt dat de verwerking van persoonsgegevens rechtmatig is voor zover de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. De laatste volzin van artikel 6 lid 1 sub f AVG voegt daaraan toe dat overheidsinstanties in het kader van de uitoefening van hun taken geen beroep kunnen doen op artikel 6 lid 1 sub f AVG.

224

In hoofdstuk 5 van dit rapport hebben wij uiteengezet dat een beroep op het gerechtvaardigd belang door overheidsinstanties alleen mogelijk is voor typisch bedrijfsmatige handelingen van die overheidsinstanties. Activiteiten zoals de onderhoudende activiteit, die toezien op of samenhangen met gereedstellen/inzet van de krijgsmacht zijn ons inziens in geen zin aan te merken als een typisch bedrijfsmatige handeling.

Gelet op het bovenstaande kan CZSK bij deze activiteit geen beroep doen op verwerking van persoonsgegevens op grond van een gerechtvaardigd belang uit artikel 6 lid 1 sub f AVG.

Concluderend merken wij op dat CZSK niet over een grondslag beschikt voor het verwerken van persoonsgegevens in deze activiteit.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	De bevoegdheid voor het verwerken van persoonsgegevens kan niet worden ontleend uit een wet in formele zin.	Het vaststellen van een wet in formele zin waaruit de bevoegdheid voor het verwerken van persoonsgegevens kan worden ontleend.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

Artikel 12 AVG bepaalt dat een betrokkene in een beknopte, transparante, begrijpelijke en gemakkelijk toegankelijke vorm en in een duidelijke, eenvoudige taal moet worden geïnformeerd over de onderwerpen genoemd in artikel 14 AVG.

Op het moment dat CZSK openbare nieuwsberichten raadpleegt en opslaat, is het voor betrokkenen, wiens persoonsgegevens in de nieuwsberichten te vinden zijn, niet duidelijk dan hun persoonsgegevens verwerkt worden. Strikt juridisch gezien moeten deze betrokkenen op grond van artikel 14 AVG ook worden geïnformeerd over de verwerking van hun persoonsgegevens. Het is echter onwenselijk als CZSK iedere betrokkene op persoonsniveau moet informeren over de verwerking van haar persoonsgegevens bij de interne verwerking van reeds gepubliceerde nieuwsberichten.

Artikel 14 lid 5 AVG biedt enkele mogelijkheden om af te wijken van de informatieplicht. Artikel 14 lid 5 sub b AVG bepaalt dat de informatieplicht uit de leden 1 tot en met 4 van artikel 14 AVG niet van toepassing is wanneer en voor zover het verstrekken van die informatie onmogelijk blijkt of onevenredig veel inspanning vergt, voor zover de in artikel 14 lid 1 AVG bedoelde verplichting de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. Wij merken op dat het (op individuele basis) informeren van iedere betrokkene een dusdanig onevenredige inspanning vergt, dat het verwerken van nieuwsberichten onmogelijk wordt. Op het moment dat een betrokkene, zoals een publiek figuur, persoonlijk is geïnformeerd, bestaat de kans dat het betreffende mediabericht al niet meer actueel is. Het bereiken en informeren van de betreffende betrokkene kan namelijk de nodige tijd in beslag nemen. Ondanks deze

onevenredige inspanning zijn wij van mening dat betrokkenen wel op algemene wijze geïnformeerd kunnen worden, door middel van de privacyverklaring op de website.

Verder vereist artikel 14 lid 5 sub b AVG dat de verwerkingsverantwoordelijke passende maatregelen neemt om de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene te beschermen, waaronder het openbaar maken van informatie. Hierover merken wij op dat CZSK de persoonsgegevens niet openbaar maakt en de informatie uit de nieuwsberichten uitsluitend gebruikt om conflictgebieden in kaart te brengen en zich voor te bereiden op eventuele missies.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
2.	Betrokkenen kunnen op algemene wijze beter worden geïnformeerd over de verwerking van nieuwsberichten door CZSK.	Het toevoegen van een passage over de verwerking van nieuwsberichten in de privacyverklaring.

Hoewel wij van mening zijn dat betrokkenen niet op individuele basis geïnformeerd hoeven worden, kunnen zij op algemene wijze wel beter worden geïnformeerd door het toevoegen van een passage in de privacyverklaring. Wij zijn dan ook van mening dat aan het beginsel van behoorlijkheid en transparantie nog niet volledig wordt voldaan.

226

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

Het raadplegen en opslaan van openbare nieuwsberichten die betrekking hebben op conflictgebieden in de wereld vindt plaats voor informatievoorziening. Respondent heeft aangegeven dat mariniers voor een missie tijdig over de benodigde relevante informatie moeten beschikken en dat niet kan worden gewacht met het informeren van de mariniers tot het moment dat een regeringsbesluit is genomen. Wij zijn van mening dit een helder omschreven doel is, waarmee wordt voldaan aan het beginsel van doelbinding.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Bij het opslaan van openbare nieuwsberichten kunnen de volgende persoonsgegevens worden verwerkt: namen van journalisten, namen/functies van personen die in het nieuwsbericht worden genoemd en andere tot personen te herleiden gegevens die in het nieuwsbericht worden genoemd, zoals ras/etnische afkomst, politieke opvattingen, godsdienst en/of levensovertuiging of strafrechtelijk verleden.

Respondent heeft aangegeven geen profielen op te stellen van leiders van groeperingen en rebellen op basis van de informatie uit openbare nieuwsberichten. Voor zover deze informatie wel relevant is voor de missie, hoopt CZSK deze informatie, voorafgaand aan de inzet, te ontvangen van de MIVD. De MIVD beschikt namelijk over de juiste bevoegdheid om deze persoonsgegevens te verwerken.

Nu CZSK uitsluitend die persoonsgegevens verwerkt die in de nieuwsberichten voorkomen, zijn wij van mening dat aan het beginsel van minimale gegevensverwerking wordt voldaan.

227

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verwerkingsverantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

De functionarissen binnen CZSK die zich bezighouden met het raadplegen en opslaan van nieuwsberichten zijn opgeleid om kritisch naar bronnen te kijken. Informatie en daarin voorkomende persoonsgegevens uit onbetrouwbare bronnen wordt niet opgeslagen.

Om de juistheid van de door CZSK verkregen kennis te controleren, stuurt CZSK voorafgaand aan de daadwerkelijke inzet een Request for Information naar de MIVD, met het verzoek om de al verkregen kennis te staven en aan te vullen en om de voor de missie benodigde persoonsgegevens te verkrijgen. De MIVD maakt voor het staven en aanvullen gebruik van andere bronnen.

Gelet hierop zijn wij van mening dat aan het beginsel van juistheid wordt voldaan.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalt, dan moeten de persoonsgegevens worden gewist.

Respondent heeft aangegeven dat relevante informatie wordt opgeslagen op de SharePoint. Hieronder vallen onder meer nieuwsberichten, publicaties en (mogelijk) relevant beeld- en geluidsmateriaal. Respondent heeft aangegeven dat er geen bewaartermijn is gekoppeld aan de nieuwsberichten, omdat van tevoren niet bekend is voor welke periode de opgeslagen informatie relevant kan zijn.

Op het moment dat de Minister van Defensie een mandaat afgeeft om over te gaan tot inzet, wordt de relevante informatie verwerkt in een briefing. Voor het verwerken van de eventuele persoonsgegevens daarin bestaat vanaf dat moment een grondslag. Andere relevante informatie wordt vanaf dat moment aangeleverd door de MIVD door middel van een Request for Information.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
3.	CZSK heeft geen bewaartermijnen vastgesteld voor de nieuwsberichten die worden opgeslagen op de SharePoint.	Het vaststellen van bewaartermijnen en deze bewaartermijnen vastleggen in de selectielijst van Defensie.

228

Gelet hierop zijn wij van mening dat er nog niet volledig wordt voldaan aan het beginsel van opslagbeperking.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De op de SharePoint opgeslagen nieuwsberichten worden beveiligd volgens het Defensiebeveiligingsbeleid. Wij zijn van mening dat hiermee wordt voldaan aan het beginsel van integriteit en vertrouwelijkheid.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG

en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Over de verwerking van persoonsgegevens in deze activiteit is niets in het verwerkingenregister terug te vinden.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
4.	De verwerking van persoonsgegevens is niet terug te vinden in het verwerkingenregister.	Het opnemen van de activiteit in het verwerkingenregister.

Wij zijn van mening dat hiermee nog niet volledig aan de verantwoordingsplicht wordt voldaan.

Conclusie

CZSK raadpleegt en slaat nieuwsberichten op die informatie bevatten over mogelijke conflictgebieden in de wereld. Op deze manier wordt het betreffende conflictgebied in kaart gebracht, zodat de mariniers bij een eventuele inzet snel kunnen worden geïnformeerd over de situatie in het conflictgebied. Hoewel deze nieuwsberichten persoonsgegevens kunnen bevatten, beschikt CZSK niet over een bevoegdheid om deze persoonsgegevens te verwerken. Voor zover CZSK een grondslag weet te creëren om persoonsgegevens te verwerken, moet er nog aandacht worden besteed aan de informatieplicht, de bewaartermijnen en het verwerkingenregister om volledig aan de verplichtingen uit de AVG te voldoen.

Activiteit 11

Omschrijving activiteit 11

De eenheid Surface Assault and Training Group (hierna: SATG) van het Commando Zeestrijdkrachten (hierna: CZSK) verzamelt data van stranden en verwerkt deze data in strandverkenningrapporten. Deze rapporten bevatten informatie over waterdieptes en bodemgesteldheid, aangevuld met foto's om de situatie te duiden.

De data die in het strandverkenningrapport wordt verwerkt, is afkomstig uit eigen metingen ter plaatse en uit openbare bronnen op het internet, waaronder satellietbeelden.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van CZSK, zoals deze uit de verschillende wet- en regelgeving blijken.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub k van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) bepaalt dat het Ministerie van Defensie de Commandant Zeestrijdkrachten als verantwoordelijke kent.

Artikel 12 AOD bepaalt over de Commandant Zeestrijdkrachten het volgende:

230

“De Commandant Zeestrijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Zeestrijdkrachten;*
- b. de gereedstelling en instandhouding van de zeestrijdkrachten;*
- c. het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Zeestrijdkrachten;*
- e. het beheer van de Kustwacht Nederland en de Kustwacht Caribische Gebied;*
- f. de advisering op het gebied van militair maritiem optreden.”*

Artikel 26 AOD bepaalt dat de Commandant Zeestrijdkrachten op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Zeestrijdkrachten 2010

Artikel 2 lid 2 sub e Subtaakbesluit Commando Zeestrijdkrachten 2010 (hierna: subtaakbesluit) bepaalt dat het Commando Zeestrijdkrachten uit een Directie Operationele Ondersteuning bestaat.

Artikel 7 subtaakbesluit bepaalt daarover het volgende:

"De directie Operationele Ondersteuning staat onder leiding van de directeur Operationele Ondersteuning die is belast met:

- a. het met inachtneming van de opdracht, planningskaders en (functionele) richtlijnen van de Commandant Zeestrijdkrachten geven van leiding aan de directie Operationele Ondersteuning;*
- b. het aanbrengen en bestendigen, binnen de opdracht en planningskaders van de Commandant Zeestrijdkrachten, van de materiële gereedheid van eenheden van het Commando Zeestrijdkrachten;*
- c. het vastleggen van de bedrijfsvoering en het aanbrengen van basisgeoefendheid tot en met het niveau van de Safety And Readiness Check 2 (SARC-2);*
- d. het facilitair ondersteunen van alle processen binnen het Commando Zeestrijdkrachten;*
- e. het coördineren van de informatievoorziening binnen het Commando Zeestrijdkrachten;*
- f. het binnen het Commando Zeestrijdkrachten optreden als aanspreekpunt voor de Defensie Materieel Organisatie;*
- g. het formuleren van de eisen aan de door de Defensie Materieel Organisatie en het Commando Dienstencentra op te leveren producten en diensten aan het Commando Zeestrijdkrachten, binnen de gestelde kaders;*
- h. het ontwikkelen en onderhouden van functionele richtlijnen - ten aanzien van het eigen terrein van verantwoordelijkheid - voor de gehele CZSK-organisatie;*
- i. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;*
- j. de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de directie Operationele Ondersteuning."*

231

Wij zijn van mening dat het opstellen van een strandverkenningsrapport kan worden gezien als het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid, zoals genoemd in artikel 7 sub i subtaakbesluit.

Toepassingsbereik AVG

Materieel toepassingsbereik

SATG verwerkt de naam van de opsteller van het strandverkenningrapport. Het noteren van een naam in een Word-bestand kwalificeert als een verwerking van persoonsgegevens op grond van artikel 2 AVG.

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

De AVG is dus wel van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

232

Gerechtvaardigd belang

Een verwerking van persoonsgegevens op grond van het gerechtvaardigd belang van de verwerkingsverantwoordelijke is volgens artikel 6 lid 1 onder f AVG toegestaan als de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke.

SATG stelt strandverkenningrapporten op, zodat mariniers veilig, snel en met het juiste materiaal van het marineschip het land kunnen bereiken. Een groot marineschip kan namelijk niet zomaar aanleggen aan de kust. Het is daarom noodzakelijk om de aanmeerlocatie van het marineschip te onderzoeken.

Respondent heeft aangegeven dat in het strandverkenningrapport geen persoonsgegevens worden opgenomen, met uitzondering van de naam van de luitenant die verantwoordelijk is voor het rapport. De naam van de luitenant wordt in het rapport opgenomen, zodat de ontvangers van het rapport weten aan wie ze eventuele vragen kunnen stellen. In dat het licht is het volgens ons noodzakelijk om dat persoonsgegeven in het strandverkenningrapport te verwerken.

Wij zijn van mening dat SATG voor het verwerken van dat persoonsgegeven een succesvol beroep kan doen op het gerechtvaardigde belang in de zin van artikel 6 lid 1 sub f AVG.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

De luitenant die zijn naam op het strandverkenningrapport zet weet dat zijn persoonsgegeven wordt verwerkt. Wij zijn van mening dat hiermee aan het beginsel van behoorlijkheid en transparantie wordt voldaan.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

233

Het doel van de verwerking is dat ontvangers van het strandverkenningrapport weten bij wie ze terecht kunnen voor vragen. In dat kader is het noodzakelijk om de naam van de luitenant te verwerken. Vereiste hierbij is echter wel dat dit doel duidelijk is voor de betrokkene. Zolang dit doel voor betrokkene duidelijk is en zijn naam in het rapport niet voor andere doeleinden wordt gebruikt, zijn wij van mening dat aan het beginsel van doelbinding wordt voldaan.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Respondent heeft aangegeven dat het strandverkenningrapport in beginsel alleen inzichtelijk is voor het eigen personeel en voor de commandanten van de marine die het strandverkenningrapport nodig hebben om aan te meren. In die gevallen zal de naam van de betreffende luitenant ook inzichtelijk zijn voor de ontvangers.

Respondent heeft aangegeven dat het strandverkenningrapport soms ook met buitenlandse mogendheden wordt gedeeld. In die gevallen wordt het strandverkenningrapport omgezet in een ander document, waarin de naam van de betreffende luitenant wordt weggelaten. Het strandverkenningrapport dat de buitenlandse mogendheid ontvangt, bevat daardoor helemaal geen persoonsgegevens meer. Eventuele vragen over het rapport kunnen zij stellen via de officiële kanalen van Defensie.

Wij zijn van mening dat hiermee aan het beginsel van minimale gegevensverwerking wordt voldaan.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Verondersteld mag worden dat de luitenant die zijn naam op het strandverkenningrapport zet het juiste persoonsgegeven verstrekt. Aan het beginsel van juistheid wordt hiermee voldaan.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalt, dan moeten de persoonsgegevens worden gewist.

Respondent heeft aangegeven dat strandverkenningrapporten worden bewaard, totdat er een nieuw rapport is. Dit betekent dat bepaalde strandverkenningrapporten vrij oud kunnen zijn. Respondent heeft aangegeven momenteel ook over strandverkenningrapporten te beschikken die twaalf jaar geleden zijn opgesteld. Een dergelijk rapport kan namelijk langdurig relevant zijn voor als er in de toekomst opnieuw aangemeerd moet worden.

Mogelijke knelpunten		Aanbevelingen
Juridisch		
1.	Hoewel de rapporten geen bewaartermijn kennen, worden de rapporten ook niet gearcheveerd, maar blijven deze lokaal opgeslagen op de werkschijf in MULAN.	Het vaststellen van bewaartermijnen voor strandverkenningrapporten in de selectielijst, waarna het rapport wordt aangeboden ter archivering. Zodra het rapport wordt gearcheveerd kan de naam van de luitenant mogelijk uit het rapport worden

		<p>verwijderd. Het rapport wordt dan centraal opgeslagen en blijft raadpleegbaar wanneer het rapport in de toekomst weer relevant is. Vanaf het moment dat de naam van de luitenant uit het rapport is verwijderd worden er geen persoonsgegevens meer verwerkt. Dat betekent dat de AVG dan niet meer van toepassing is en dat het rapport (zonder de naam van de luitenant) in principe oneindig bewaard mag worden.</p>
--	--	--

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Respondent heeft aangegeven dat de strandverkenningrapporten op de lokale schijf in MULAN worden opgeslagen. Deze rapporten zijn alleen toegankelijk voor daartoe geautoriseerd personeel. De werkomgeving is daarnaast onderworpen aan het Defensie Beveiligingsbeleid. Gelet hierop concluderen wij dat aan de vereisten van integriteit en vertrouwelijkheid wordt voldaan.

235

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Respondent heeft aangegeven dat de verwerking van persoonsgegevens in deze activiteit niet is opgenomen in het verwerkingsregister van Defensie. Op Texel staan er twee activiteiten in het verwerkingsregister, namelijk de verwerking van namen en contactgegevens voor een belboom wanneer er paniek uitbreekt en de verwerking van namen voor de autorisatielijst. Dit zijn beide verwerkingen die worden uitgevoerd door de personeelsfunctionaris.

Hoewel er geringe risico's kleven aan de verwerking van de naam van de luitenant in een strandverkenningrapport, zijn wij van mening dat deze

verwerking wel kan worden opgenomen in het verwerkingenregister van Defensie.

Mogelijke knelpunten		Aanbevelingen
Juridisch		
2.	De verwerking van de naam van de luitenant in een strandverkenningrapport is nog niet expliciet opgenomen in het verwerkingenregister van Defensie.	Het opnemen van deze activiteit in het verwerkingenregister van Defensie.

Conclusie

SATG beschikt volgens ons over een grondslag om persoonsgegevens te verwerken in haar strandverkenningrapporten. Over het algemeen wordt ook aan de overige beginselen uit artikel 5 AVG voldaan. Alleen op het gebied van opslagbeperking valt nog winst te behalen door bewaartermijnen vast te stellen voor de strandverkenningrapporten en deze rapporten gecentraliseerd te archiveren.

Activiteit 12

Omschrijving activiteit 12

De Defensie Materieel Organisatie (hierna: DMO) houdt zich bezig met aankoop, instandhouding en verkoop van defensiematerieel. Dit voert DMO in een defensiebreed spectrum uit en varieert van de aankoop van een bureaustoel tot een F-35 straaljager.

De afdeling Inkoop van de DMO legt ten behoeve van contractmanagement zakelijke gegevens van leveranciers en eindklanten vast in SAP M&F en Negometrix. Daarbij worden ook persoonsgegevens vastgelegd ter uitvoering van contracten met leveranciers en eindklanten.

Er wordt momenteel gewerkt aan een (gedeeltelijke) migratie naar een nieuw systeem in een online cloud-omgeving (SAP 4 HANA module Ariba), dat naar verwachting in 2023 uitgerold zal worden. Voor aanbestedingen is van belang dat leveranciers toegang kunnen krijgen tot bepaalde informatie, zoals de uitvraag, te ondertekenen contracten en daarbij behorende informatie zoals toelichtingen/instructies en dergelijke. Dit is bij het huidige systeem nog niet mogelijk, omdat het op het interne (beveiligde) netwerk van Defensie draait. Leveranciers zullen enkel onder bepaalde voorwaarden tot specifieke onderdelen van SAP Ariba autorisatie krijgen conform het Defensie Beveiligingsbeleid (DBB).

237

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DMO, zoals deze uit de verschillende wet- en regelgeving blijken.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub p van het Algemeen organisatiebesluit Defensie 2021 (hierna: AOD) bepaalt dat het Ministerie van Defensie de Directeur Defensie Materieel Organisatie als verantwoordelijke kent.

Artikel 17 AOD bepaalt over de Directeur Defensie Materieel Organisatie het volgende:

“De Directeur Defensie Materieel Organisatie is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van ambtelijke leiding aan de Defensie Materieel Organisatie;*
- b. het binnen de kaders leveren van ondersteunende producten en diensten op het gebied van materieel en IV/ICT dienstverlening en het waarborgen van de kwaliteit van deze dienstverlening;*

- c. wapensysteemmanagement;
- d. het functioneel aansturen van de verwerving en de centrale verwerving van producten en diensten boven M€ 5;
- e. materieelprojecten binnen de kaders van het defensiematerieelproces (DMP);
- f. de afstoting van materieel;
- g. de advisering op het toegewezen functiegebied en het van daaruit ondersteunen van de overige defensieonderdelen."

De aankoop, instandhouding en verkoop van defensiematerieel kan worden geschaard onder de taken uit artikel 17 a t/m g AOD.

Toepassingsbereik AVG

Materieel toepassingsbereik

Bij deze activiteit komt het voor dat de afdeling Inkoop (zakelijke) contactgegevens van eindklanten vastlegt in SAP, zoals namen van contactpersonen, correspondentieadressen en zakelijke e-mailadressen. Namen zijn persoonsgegevens en een correspondentieadres en zakelijk e-mailadres kunnen ook persoonsgegevens zijn, wanneer dit herleidbaar is tot een individu. Er is bij deze activiteit daarom sprake van verwerking van persoonsgegevens, waardoor de AVG op grond van artikel 2 van toepassing is.¹⁰⁴

238

Territoriaal toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland en de verwerking van persoonsgegevens bij deze activiteit ook plaatsvindt binnen Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

Kortom, de AVG is van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is.

¹⁰⁴ Op een van de uitzonderingen uit artikel 2 AVG kan geen beroep worden gedaan, omdat DMO geen krijgsmachtonderdeel is.

Uitvoering overeenkomst

De afdeling Inkoop van DMO mag persoonsgegevens van leveranciers en eindklanten rechtsgeldig verwerken voor zover dit strikt noodzakelijk is voor het aangaan (instemming) en de uitvoering van een overeenkomst (artikel 6 lid 1 sub b AVG). Bijvoorbeeld om in overleg te treden over een (concept)overeenkomst of om deze ter inzage of accordering naar een leverancier te sturen, is het gebruik van (minimaal) een e-mailadres of telefoonnummer noodzakelijk.

Gerechtvaardigd belang

Uit overweging 47 van de AVG blijkt dat overheidsinstanties geen beroep mogen doen op het gerechtvaardigd belang in het kader van de uitvoering van hun taken. Een beroep hierop is voor een overheidsinstantie alleen mogelijk voor de verwerking van persoonsgegevens bij typisch bedrijfsmatige handelingen. Wij zijn van mening dat de aankoop, instandhouding en verkoop van defensiematerieel kwalificeert als een typisch bedrijfsmatige handeling voor het Ministerie van Defensie. Dit brengt met zich mee dat DMO voor de verwerking van persoonsgegevens bij de aankoop, instandhouding en verkoop van defensiematerieel een beroep kan doen op het gerechtvaardigde belang uit artikel 6 lid 1 sub f AVG. Voor een geslaagd beroep op een gerechtvaardigd belang is een belangenafweging noodzakelijk. Deze belangenafweging moet Defensie uitvoeren waarbij er aandacht wordt besteed aan het gerechtvaardigde belang van Defensie bij verwerking van persoonsgegevens en het daar tegenoverstaande belang van een individu en de inbreuk op diens rechten en vrijheden. Alleen als deze belangenafweging in het voordeel van Defensie uitvalt, kan er een beroep worden gedaan op deze grondslag. De belangenafweging moet ook worden vastgelegd, om te kunnen voldoen aan de verantwoordingsplicht uit artikel 5 AVG.

239

Wij concluderen dat aan het beginsel van rechtmatigheid wordt voldaan.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

Op het moment dat leveranciers en eindklanten bij deze activiteit actief hun persoonsgegevens aanleveren bij Inkoop, is het evident dat zij ermee bekend zijn dat die persoonsgegevens voor het uitvoeren van deze activiteit door DMO

worden verwerkt. Wij concluderen daarom dat aan het beginsel van behoorlijkheid en transparantie wordt voldaan.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel. Het doel van de verwerking van persoonsgegevens bij deze activiteit is om uitvoering te kunnen geven aan overeenkomsten die DMO met eindklanten en leveranciers aangaat. Wij zijn van oordeel dat sprake is van een gerechtvaardigd doel. Respondent heeft aangegeven dat in de modelcontracten is opgenomen welke (persoons)gegevens moeten worden ingevuld. Hierdoor is bij betrokkenen ook duidelijk welke persoonsgegevens van hen worden verwerkt. Hoewel wij bij het onderzoek geen inzage hebben gehad in een contract, heeft respondent aangegeven dat in contracten duidelijk het doel van de verwerking wordt beschreven.

Verdere verwerkingen

Uit het interview met respondenten kwam naar voren dat reeds vastgelegde contactgegevens van leveranciers in SAP ook werden gebruikt om eventuele nieuwe contracten aan te gaan met de betreffende leveranciers. In het kader van de AVG is dan sprake van een zogeheten *verdere* verwerking. Opmerking verdient dat deze verdere verwerking verenigbaar moet zijn met het oorspronkelijke verwerkingsdoel. Gelet op het doel van deze verdere verwerking, is onzes inziens sprake van een verdere verwerking die verenigbaar is met het oorspronkelijke verwerkingsdoel (uitvoering van een overeenkomst). Hierbij weegt ook de omstandigheid mee dat leveranciers, waarmee DMO eerder zaken heeft gedaan, kunnen verwachten dat hun (persoons)gegevens opnieuw worden verwerkt om een eventuele nieuwe overeenkomst aan te gaan.

Wij concluderen dat aan het beginsel van doelbinding wordt voldaan.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt.

Respondent heeft aangegeven dat enkel (persoons)gegevens worden verwerkt die voor het beoogde doel noodzakelijk zijn. Dit hebben wij niet kunnen verifiëren, bijvoorbeeld door inzage te krijgen in een inkooporder. Wij gaan

daarom uit van hetgeen respondent heeft aangegeven. Wij concluderen op basis daarvan dat het beginsel van minimale gegevensverwerking wordt nageleefd.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Bij eventuele wijzigingen in (persoons)gegevens kunnen leveranciers/eindklanten terecht bij de betreffende contractmanager. Ook kunnen zij wijzigingen doorgeven via het portaal op defensie.nl/privacy. Inkopers kunnen eventuele wijzigingen in (persoons)gegevens doorgeven via een daarvoor beschikbaar gesteld webformulier. Behalve voor betrokkenen, is het in het kader van de uitvoering van deze activiteit ook in het grootste belang voor de afdeling Inkoop zelf dat (persoons)gegevens juist en actueel zijn.

Wij concluderen dat aan het juistheidsbeginsel wordt voldaan.

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalst, dan moeten de persoonsgegevens worden gewist.

Documenten waarin persoonsgegevens staan, zoals een overeenkomst, worden als DIR bestand opgeslagen in SAP M&F. In deze DIR bestanden wordt ook een bewaartermijn vastgelegd. De standaard bewaartermijn is 7 jaren, maar kan afwijken (zie hierna over de Selectielijst).

Volgens de Selectielijst Defensie, volgnummer 10.3.2 worden gegevens met betrekking tot de werving van materieel bewaard tot 10 jaar na buitengebruikstelling van het betreffende materieel. Daarnaast geldt voor gegevens over belangrijk materieel de aanduiding SA-B5. Dit houdt onder andere in dat wanneer bij deze registraties persoonsgegevens voorkomen, op voorhand wordt bepaald of de gegevens als dusdanig of in geanonimiseerde/gepseudonimiseerde¹⁰⁵ vorm bewaard worden.

Ons inziens is in voldoende mate sprake van opslagbeperking.

¹⁰⁵ Voor de definities van en het onderscheid tussen geanonimiseerde gegevens en gepseudonimiseerde gegevens, zie de begrippenlijst in *Bijlage 5* van dit rapport.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Autorisatie tot de verschillende onderdelen van de systemen binnen het inkoopproces is 'role based' ingericht. Hierdoor hebben alleen de inkoopmedewerkers die de (persoons)gegevens voor de uitvoering van het inkoopproces nodig hebben, toegang tot die gegevens.

Respondent heeft toegelicht dat privacybewustzijn bij medewerkers van de afdeling Inkoop wordt gecreëerd. Dit gebeurt door middel van voorlichtingen, kennissessies, interne publicaties en nieuwsbrieven (algemeen en specifiek gericht op Inkoop) en middels toelichtingen en handleidingen bij modelcontracten. Wel gaf respondent tijdens het interview aan dat het voor medewerkers van de afdeling Inkoop niet altijd helemaal duidelijk is wat hem of haar te doen staat als het om de AVG gaat. Bijvoorbeeld wat voor analyse moet worden gemaakt wanneer persoonsgegevens worden verwerkt, waar op moet worden gelet wanneer persoonsgegevens worden verwerkt en hoe een verwerkingsovereenkomst er precies uit ziet. Respondent gaf aan dat, waarschijnlijk in verband met de beschikbare capaciteit binnen DMO, de AVG niet altijd 'on top of mind' staat.

242

De verwerking van persoonsgegevens in SAP vindt plaats op het eigen netwerk van Defensie (MULAN). Respondent gaf aan dat bij ingebruikname van de cloudomgeving van SAP Ariba enkel ongerubriceerde gegevens zullen worden verwerkt. Daarnaast is op deze systemen het Defensie Beveiligingsbeleid (DBB) van toepassing.

Wij vroegen respondent in verband met de beoogde ingebruikname van de cloud-omgeving van SAP Ariba of DMO bekend is met de uitspraak van het Hof van Justitie van de Europese Unie van 16 juli 2020 (Schrems II). Respondent heeft toegelicht dat de problematiek die speelt in geval van doorgifte van persoonsgegevens buiten de Europese Economische Ruimte (hierna: EER) wordt meegenomen bij de ontwikkeling van het nieuwe systeem en in het DPIA-proces. Wij zijn van mening dat bij de beoogde ingebruikname van SAP Ariba op adequate wijze rekening wordt gehouden met de geldende vereisten voor doorgifte van persoonsgegevens buiten de EER.

Ter toelichting: de AVG stelt dat persoonsgegevens niet zomaar mogen worden doorgegeven aan personen of organisaties die gevestigd zijn in landen buiten de EER (derde landen), zoals de Verenigde Staten (hierna: VS). Dit mag alleen

als in die derde landen het door de AVG gewaarborgde beveiligingsniveau voor persoonsgegevens niet wordt ondermijnd. De AVG noemt een aantal mogelijkheden om dit te bewerkstelligen. Zo werd doorgifte van persoonsgegevens naar de VS bewerkstelligt door middel van een adequaatheidsbesluit (Privacy Shield-verdrag tussen EU en VS) en modelcontracten (standaard contractual clauses of SCC's). Het Hof van Justitie van de Europese Unie (HvJEU) oordeelde echter dat doorgifte van persoonsgegevens op basis van het Privacy Shield en SCC's onvoldoende waarborgen bood. Gevolg: doorgifte van persoonsgegevens naar de VS (en veel andere derde landen) is onrechtmatig. Op het moment van het schrijven van dit onderzoek hebben de Europese Commissie en de Verenigde Staten aangekondigd dat zij een principeakkoord hebben bereikt over een Trans-Atlantic Privacy Framework, die een oplossing beoogt te bieden voor doorgifte van persoonsgegevens naar de Verenigde Staten.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	Bij de beoogde ingebruikname van SAP Ariba vindt mogelijk doorgifte van persoonsgegevens plaats buiten de EER.	Daar waar mogelijk, doorgifte van persoonsgegevens buiten de EER zoveel mogelijk voorkomen. Voor zover doorgifte buiten de EER zal plaatsvinden, dienen de vereisten voor doorgifte buiten de EER te worden nageleefd. Hieronder valt onder meer de actualisatie van de DPIA (SAP).
<i>Organisatorisch</i>		
2.	Mogelijk capaciteitsissue waardoor kennisvergaring over en inrichting van werkzaamheden conform de AVG mogelijk in mindere mate prioriteit krijgt. In dat geval kan dit leiden tot een verhoogd risico op privacy-/beveiligingsinbreuk.	Creëren van capaciteit en/of het creëren van prioriteit voor kennisvergaring en privacybewustzijn.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

Respondent heeft aangegeven dat data die bij deze activiteit wordt verwerkt als onderdeel van het totaalproces is opgenomen in het AVG verwerkingsregister van de Rijksoverheid en is gepubliceerd. Wij zijn van oordeel dat hiermee aan de verantwoordingsplicht wordt voldaan.

Conclusie

DMO beschikt volgens ons over een grondslag om persoonsgegevens te verwerken. Enerzijds kan DMO aanvoeren dat het verwerken van persoonsgegevens noodzakelijk is om de overeenkomst uit te voeren. Anderzijds kan DMO aanvoeren dat het verwerken van persoonsgegevens noodzakelijk is voor het gerechtvaardigde belang van DMO, mits de daarvoor vereiste belangenafweging in het voordeel uitvalt van DMO. Bij de verdere beoordeling van de activiteit hebben wij twee knelpuntenesignaleerd. In de eerste plaats vindt er bij de beoogde ingebruikname van SAP Ariba mogelijk uitwisseling van persoonsgegevens plaats buiten de EER. In de tweede plaats is er mogelijk sprake van een capaciteitsprobleem, waardoor kennisvergaring over en inrichting van werkzaamheden conform de AVG mogelijk in mindere mate prioriteit krijgt. Ten aanzien van deze knelpunten hebben wij enkele aanbevelingen geformuleerd.

Activiteit 13

Omschrijving activiteit 13

Het Joint Informatievoorziening Commando (hierna: JIVC) houdt zich bezig met het ontwikkelen van systemen voor en het leveren van data aan klanten. Deze 'klanten' zijn de interne onderdelen binnen Defensie. Ook houdt JIVC zich bezig met experimenten op het gebied van IT (in de breedste zin van het woord).

JIVC is vooral faciliterend en heeft geen tot weinig zicht op hoe klanten vervolgens omgaan met de verwerking van persoonsgegevens op die systemen. JIVC maakt bijvoorbeeld simulatieomgevingen of bepaalde systemen en voert data-analyses uit.

Kennis, Innovatie, eXperimenten en Simulatie (hierna: KIXS)

KIXS is de ICT-innovatieafdeling van JIVC. Onderdeel van KIXS zijn:

- Afdeling innovatie: binnen deze afdeling voert KIXS veel experimenten op IT-gebied uit. KIXS onderzoekt bijvoorbeeld of het mogelijk is om bepaalde systemen te bouwen. Aan de hand van fictieve datasets test KIXS deze systemen.
- Afdeling datalab: het datalab bestaat uit ongeveer 25 data engineers. Deze engineers maken in opdracht van verschillende Defensieonderdelen systemen of platformen.

245

Het uitgangspunt is dat KIXS geen persoonsgegevens verwerkt. Ook bij grote datasets gebruikt deze afdeling fictieve data om te testen of bepaalde systemen werken. Momenteel loopt er intern een inventarisatie om te onderzoeken waar eventueel toch persoonsgegevens worden verwerkt. Dit is gericht op de vraag of KIXS daarbij binnen de kaders van de geldende wet- en regelgeving handelt.

Het is lastig om de werkzaamheden van KIXS af te kaderen. Dit komt omdat KIXS op experimentele (gelet op het innoverende karakter) basis werkt. Hierdoor is het op voorhand vaak moeilijk zeggen wat wel en wat niet kan. Dit heeft ten gevolge dat het niet mogelijk is om op voorhand een allesomvattende werkhandleiding te schrijven waarmee een aanvrager uit de voeten kan. Het bouwen van systemen vindt niet alleen plaats bij KIXS. KIXS richt zich in deze zin vooral op innovatie en research & development.

JIVC – bouwen van systemen

JIVC bouwt los van KIXS het grootste deel van de systemen voor klanten. Bij het bouwen van die systemen verwerkt JIVC wel persoonsgegevens. Uitgangspunt is dat JIVC alleen persoonsgegevens verwerkt bij het bouwen van een systeem als dit in opdracht van een klant wordt gedaan. Het verwerken van persoonsgegevens is onvermijdelijk bij het bouwen van een systeem. Op

voorhand vindt een intakegesprek met de klant plaats. Bij dit gesprek gebruiken JIVC en de klant de Aanwijzing Kaders Data (Science) Projecten (hierna: normenkader).¹⁰⁶ In het normenkader staan naast privacyaspecten ook andere zaken zoals wie voor welk aspect verantwoordelijk is. De verantwoordelijkheid voor het verwerken van persoonsgegevens ligt hierbij bij de klant. De klant voert in veel gevallen dus zelf een Data Protection Impact Assessment (hierna: DPIA) uit en is ook verantwoordelijk om de beginselen uit de Algemene verordening gegevensbescherming (hierna: AVG) in acht te nemen. JIVC is wel verantwoordelijk voor het security-gedeelte aangezien de systemen op het netwerk van JIVC staan. Het bouwen van systemen vindt alleen intern plaats en is daarmee onderdeel van de interne bedrijfsvoering van Defensie.

Bij het bouwen van systemen voldoet JIVC aan de normen van D300. Dit is een set aan beveiligingsmaatregelen waardoor JIVC ook de privacyrisico's dekt. Ook houdt JIVC rekening met het Defensie Beveiligingsbeleid (hierna: DBB).

Leveren van datasets

Naast het bouwen van systemen en platforms levert JIVC incidenteel op aanvraag ook bepaalde datasets. Denk daarbij aan personeelsbestanden van bepaalde Defensieonderdelen. JIVC levert deze datasets alleen als de daarvoor verantwoordelijke personen toestemming geven.

246

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van JIVC, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 44 Grondwet (hierna: GW) bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministers staan onder leiding van een minister. Bij koninklijk besluit is het Ministerie van Defensie ingesteld.¹⁰⁷

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub p van het AOD bepaalt dat het Ministerie van Defensie de Directeur Defensie Materieel Organisatie als verantwoordelijke kent.

¹⁰⁶ Aanwijzing Kaders Data (Science) Projecten, kenmerk DGB-CIO-101.

¹⁰⁷ Koninklijk besluit van 19 mei 1959, nr. 128104, houdende wijziging in de taakverdeling, samenvoeging en naamswijziging van departementen.

Artikel 17 AOD bepaalt over de Directeur Defensie Materieel Organisatie het volgende:

"De Directeur Defensie Materieel Organisatie is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van ambtelijke leiding aan de Defensie Materieel Organisatie;*
- b. het binnen de kaders leveren van ondersteunende producten en diensten op het gebied van materieel en IV/ICT dienstverlening en het waarborgen van de kwaliteit van deze dienstverlening;*
- c. wapensysteemmanagement;*
- d. het functioneel aansturen van de verwerving en de centrale verwerving van producten en diensten boven M€ 5;*
- e. materieelprojecten binnen de kaders van het defensiematerieelproces (DMP);*
- f. de afstoting van materieel;*
- g. de advisering op het toegewezen functiegebied en het van daaruit ondersteunen van de overige defensieonderdelen."*

Artikel 26 AOD bepaalt dat de Directeur Defensie Materieel Organisatie op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leiding geeft.

Subtaakbesluit Defensie Materieel Organisatie 2013

247

Artikel 1 sub f van het subtaakbesluit Defensie Materieel Organisatie 2013 (hierna: subtaakbesluit) bepaalt dat JIVC onder Defensie Materieel Organisatie valt.

Artikel 7 van het subtaakbesluit kent de volgende taken toe aan de Directeur JIVC:

"Het Joint Informatievoorzieningscommando staat onder leiding van de Directeur JIVC die is belast met:

- a. Het met inachtneming van de aanwijzingen en richtlijnen van de Directeur Defensie Materieel Organisatie geven van ambtelijke leiding aan het JIVC;*
- b. Het met inachtneming van de regeling agentschappen van de Minister van Financiën invulling geven aan de rol van opdrachtgever voor het agentschap Operations voor het laten leveren van IV- en ICT- producten- en diensten;*
- c. Het leveren en instand houden van IV- ICT- en Informatiebeheer producten en diensten;*
- d. Het reguleren van vraag en aanbod om tot goede en betaalbare IV- voorzieningen te komen;*
- e. Het proactief zorgdragen voor innovatieve producten en diensten op IV- gebied;*

- f. *Het zorgdragen voor voorspelbare kwaliteit, tijd en kosten van de geleverde diensten;*
- g. *Het zorgdragen voor de doelmatige inrichting, de bedrijfsvoering en het interne beheer van het JIVC.”*

Op grond van het subtaakbesluit (in het bijzonder artikel 7 sub c) is het bouwen van systemen door JIVC te kwalificeren als een taak van JIVC. Het innoverende gedeelte waar KIXS zich mee bezighoudt is op grond van artikel 7 sub e subtaakbesluit aan te merken als een taak van JIVC.

Toepassingsbereik AVG

Materieel toepassingsgebied

Bij deze activiteit verwerkt JIVC bij bepaalde werkzaamheden persoonsgegevens. Deze verwerkingen vinden op verschillende momenten plaats:

Het ontwikkelen van systemen in opdracht van klanten. De verantwoordelijkheid voor de verwerking van persoonsgegevens ligt hierbij niet bij JIVC;

Aanleveren van datasets aan Defensieonderdelen (continue of incidenteel).

Het uitgangspunt bij KIXS is om bij het innovatiegedeelte geen persoonsgegevens te verwerken. Als een klant een systeem laat ontwikkelen door JIVC, dan verwerkt JIVC vaak wél persoonsgegevens. De (interne) verantwoordelijkheid voor de verwerking ligt niet bij JIVC. De systemen worden namelijk onder verantwoordelijkheid van de klant geïnitieerd. Er is geen indicatie dat JIVC persoonsgegevens verwerkt in eigen beheer voor zelf opgestelde doelen.

248

Aangezien JIVC persoonsgegevens verwerkt valt deze activiteit op grond van artikel 2 AVG binnen het materieel toepassingsbereik van de AVG.

Territoriaal toepassingsgebied

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriaal toepassingsgebied van de AVG.

De AVG is dus van toepassing op deze activiteit.

Beoordeling activiteit

Artikel 5 AVG bepaalt dat de verwerkingsverantwoordelijke bij de verwerking van persoonsgegevens aan verschillende beginselen moet voldoen. Het gaat om de volgende beginselen:

- Rechtmatigheid;
- Behoorlijkheid & transparantie;

- Doelbinding;
- Minimale gegevensverwerking;
- Opslagbeperking;
- Juistheid;
- Integriteit & vertrouwelijkheid;
- Verantwoordingsplicht.

Het bijzondere aan de werkwijze bij deze activiteit is dat de klant aan deze beginselen moet voldoen en ze moet naleven. De klant is namelijk verantwoordelijk voor de verwerking van persoonsgegevens bij het bouwen van een systeem. In dat kader voert de klant ook – indien nodig – een DPIA uit. Dat wil niet zeggen dat JIVC niet mee wil/kan denken bij de invulling van deze beginselen in de breedste zin van het woord. Denk hierbij aan de beginselen van privacy by design en privacy by default.¹⁰⁸ JIVC borgt het beginsel privacy by design. Dit komt omdat JIVC de normen van D300 implementeert. Ook denken medewerkers bij het bouwen van een systeem mee en geven zij aan of bepaalde wensen van de klant wel of juist niet in lijn zijn met de AVG. Dit is onderdeel van het beginsel privacy by default.

Mogelijke knelpunten

Aan een toetsing van artikel 5 AVG komen we bij deze activiteit vanwege de positie van de verwerkingsverantwoordelijke niet toe. Ondanks dat JIVC niet de verantwoordelijke is voor de verwerking van persoonsgegevens in de systemen, zijn er mogelijk wel knelpunten:

Mogelijke knelpunten		Aanbevelingen
<i>Organisatorisch</i>		
1.	JIVC heeft waarschijnlijk te weinig inzicht of de klant aan de voor- en achterkant voldoende rekening houdt met de privacyregelgeving. De klant heeft een grondslag nodig om persoonsgegevens te verwerken in het te bouwen systeem. In het kader van de rechtmatigheid wordt een knelpunt ervaren bij JIVC. Vaak levert de klant bij het ontwikkelen van bepaalde systemen wel een DPIA aan, maar onduidelijk is hoe deze tot	<p>Richt procedures in waarbij aandacht wordt besteed aan rollen en verantwoordelijkheden tussen Defensieonderdelen en JIVC. Denk hierbij aan het opstellen van een werkhandleiding.</p> <p>Zo krijgt JIVC meer inzicht of de systemen voldoen aan de geldende wet- en regelgeving en wordt het zicht op de voor- en achterkant van het proces vergroot.</p>

¹⁰⁸ Artikel 25 AVG.

	<p>stand is gekomen en of er periodiek een controle plaatsvindt.</p> <p>Ook ontvangt JIVC verzoeken voor het aanleveren van data(analyses). Denk hierbij aan het leveren van een personeelsbestanden van een Defensieonderdeel. Onduidelijk is of zo'n verzoek altijd rechtmatig is en wat hiervoor de voorwaarden zijn. Dit komt omdat JIVC onvoldoende inzicht heeft in de manier waarop een verzoek bij de klant tot stand is gekomen.</p> <p>Bij het aanleveren van data na een verzoek stelt JIVC in dat bepaalde data automatisch periodiek wordt verstuurd. Dit gaat in sommige gevallen zelfs enkele jaren door. Onduidelijk is of bij de ontvanger ook periodiek wordt gekeken of de persoonsgegevens nog noodzakelijk zijn voor het doel waarvoor zij oorspronkelijk zijn opgevraagd.</p> <p>JIVC ervaart dus als knelpunt dat ze te weinig inzicht hebben in het gehele proces en dat zij enkel de opdracht krijgen om een systeem te maken of een dataset aan te leveren, zonder dat JIVC weet of dit aan de voor- en achterkant goed is ingeregeld en of de AVG wordt nageleefd.</p>	
2.	Er is een capaciteitstekort op het gebied van kennis van de geldende privacy (en	We hebben de volgende aanbevelingen als het gaat om dit knelpunt:

	<p>aanverwante) wet- en regelgeving binnen JIVC. Dit heeft de verschillende (geconstateerde) consequenties tot gevolg:</p> <p>Het verwerkingsregister is niet actueel. Dit komt omdat er te weinig tijd is om dit bij te werken, oude verwerkingen uit het systeem te halen en nieuwe verwerkingen in het systeem op te nemen.</p> <p>In sommige gevallen ervaren medewerkers van JIVC een 'grijs gebied' over wat wel en wat geen persoonsgegevens zijn. Dit kan soms het verschil zijn of JIVC wel of geen data-analyse uitvoert. Een voorbeeld van dit grijze gebied is een droneregistratienummer. Voor medewerkers is het onduidelijk of dit wel of geen persoonsgegeven is. Er is onvoldoende capaciteit aanwezig om alle vragen tijdig te beantwoorden en/of medewerkers te ondersteunen als het gaat om privacyvraagstukken.</p>	<p>Zorg voor voldoende kennis bij medewerkers over de AVG;</p> <p>Zorg voor voldoende personeel dat zich bezighoudt met privacy gerelateerde vraagstukken, zoals het bijhouden van het verwerkingsregister en het uitvoeren van DPIA's. Volgens de respondenten is er momenteel te weinig capaciteit;</p> <p>Richt een werkproces in om te zorgen voor een actueel verwerkingsregister en houd hiermee rekening in de planning;</p> <p>Stel een lijst op met voorbeelden van (verwerkingen van) persoonsgegevens;</p> <p>Zorg voor korte lijnen tussen bijvoorbeeld de FG, privacy coördinatoren en medewerkers van JIVC/KIXS, waarbij met enige regelmaat deze problematiek wordt besproken. Het moet voor medewerkers helder zijn waar ze terecht kunnen met privacyvraagstukken. In het verlengde hiervan komt de FG binnenkort een lezing geven bij medewerkers van JIVC.</p>
<i>Ethisch</i>		
3.	<p>Door de politieke druk schiet personeel van JIVC in de kramp. Zo denkt personeel van JIVC dat ze bepaalde data-analyses niet uit kunnen voeren, terwijl er bij veel data-analyses geen persoonsgegevens worden verwerkt. Denk aan luchtmetingen en het meten van vliegbewegingen. Er kan dus heel veel met data, ook als het</p>	<p>Door het vergroten van de bewustwording van de AVG weet personeel van JIVC wat de mogelijkheden zijn. Zo voert het personeel meer data-analyses uit en wordt de boot minder vaak gemist. Breng het onderwerp privacy daarnaast blijvend onder de aandacht van medewerkers. Geef bijvoorbeeld regelmatig privacy bewustwordingstrainingen</p>

	<p>geen persoonsgegevens zijn.</p> <p>Personeel is naar aanleiding van LMC erg terughoudend.</p> <p>Hierdoor loopt JIVC kansen mis en voert JIVC data-analyses niet uit waar zij dit wel kunnen.</p>	
--	--	--

Conclusie

De activiteit kan doorgang vinden op de huidige manier, maar er zijn mogelijk wel aanbevelingen. Zeker op het gebied van kennis van de AVG en medewerkers die zich bezig houden met privacy. De capaciteit lijkt op dit moment onvoldoende te zijn. Zo staan activiteiten niet in het verwerkingsregister waar dit wel moet en spelen er af en toe vraagstukken of iets wel of geen persoonsgegeven is. Hierdoor voert JIVC/KIXS soms geen data-analyses uit. Door de capaciteit te vergroten wordt dit mogelijke knelpunt verholpen. Ook is het raadzaam om structureel privacy trainingen te geven om de bewustwording onder de medewerkers te vergroten. Volgens de respondenten speelt er op dit moment een 'LMC-angst'. Door de kennis en bewustwording te vergroten wordt hier op ingespeeld.

Indien het als knelpunt wordt ervaren dat JIVC te weinig zicht heeft op de voor- en achterkant van het proces bij het bouwen van systemen of het leveren van data, is het raadzaam om de werkprocessen te evalueren en waar nodig te verbeteren.

Deze aanbevelingen blokkeren de doorgang van deze activiteit echter niet. Daarom krijgt deze activiteit de kleur groen.

Activiteit 14A

Omschrijving activiteit 14A

Het Joint Informatievoorziening Commando (hierna: JIVC) is het interne IT-bedrijf van Defensie. Onderdeel van JIVC is het Defensie Cyber Security Centrum (hierna: DCSC). DCSC houdt zich onder andere bezig met het voorkomen en detecteren van cyberaanvallen. Het doel hiervan is het beschermen van de interne netwerken en systemen van Defensie. Deze activiteiten hebben een defensief karakter. Dit in tegenstelling tot het Defensieonderdeel Defensie Cyber Commando (hierna: DCC), waar de activiteiten meer gericht zijn op de offensieve cybercapaciteit van Defensie. DCSC voert verschillende activiteiten uit om de netwerken en systemen te beschermen.

Activiteit 14A gaat over monitoring (actief) en logging (reactief). Het doel hiervan is om (eventuele) afwijkingen van het normale patroon zichtbaar te maken. Het systeem maakt deze afwijkingen zichtbaar doordat bepaalde regels en triggers zijn ingesteld. Vervolgens onderzoeken en analyseren gespecialiseerde analisten van DCSC deze afwijkingen, onder meer om *false positives* eruit te filteren. Bij noemenswaardige afwijkingen, stelt een analist een rapport op aan de hand van de bevindingen. Het monitoren en loggen vindt intern plaats en is daarmee onderdeel van de bedrijfsvoering. Het gaat hierbij om indirect herleidbare persoonsgegevens en gepseudonimiseerde persoonsgegevens. Gepseudonimiseerde persoonsgegevens niet hetzelfde als *anonieme* persoonsgegevens. Bij anonieme persoonsgegevens is de betrokkene niet (meer) te herleiden en is de Algemene Verordening Gegevensbescherming (hierna: AVG) niet van toepassing. In het geval van indirect herleidbare en gepseudonimiseerde persoonsgegevens is dat niet het geval en is de AVG van toepassing.¹⁰⁹

253

Het doel van het verzamelen van persoonsgegevens bij deze activiteit is om Defensiepersoneel dat (on)bewust mogelijk schadelijke handelingen verricht (eventueel) hierop aan te spreken, of het cyberincident te volgen in het systeem. Momenteel voert DCSC een Data Protection Impact Assessment (hierna: DPIA) uit op de bouwstenen van DCSC. Deze DPIA bevindt zich in een vergevorderd stadium. Voor de beoordeling van de activiteit hebben wij op 10 februari 2022 inzage verkregen in de DPIA.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van JIVC-DCSC, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het

¹⁰⁹ Zie artikel 4 sub 5 AVG.

Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 44 Grondwet (hierna: GW) bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministers staan onder leiding van een minister. Bij koninklijk besluit is het Ministerie van Defensie ingesteld.¹¹⁰

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub p van het AOD bepaalt dat het Ministerie van Defensie de Directeur Defensie Materieel Organisatie als verantwoordelijke kent.

Artikel 17 AOD bepaalt over de Directeur Defensie Materieel Organisatie het volgende:

“De Directeur Defensie Materieel Organisatie is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van ambtelijke leiding aan de Defensie Materieel Organisatie;*
- b. het binnen de kaders leveren van ondersteunende producten en diensten op het gebied van materieel en IV/ICT dienstverlening en het waarborgen van de kwaliteit van deze dienstverlening;*
- c. wapensysteemmanagement;*
- d. het functioneel aansturen van de verwerving en de centrale verwerving van producten en diensten boven M€ 5;*
- e. materieelprojecten binnen de kaders van het defensiematerieelproces (DMP);*
- f. de afstoting van materieel;*
- g. de advisering op het toegewezen functiegebied en het van daaruit ondersteunen van de overige defensieonderdelen.”*

254

Artikel 26 AOD bepaalt dat de Directeur Defensie Materieel Organisatie op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leiding geeft.

Subtaakbesluit Defensie Materieel Organisatie 2013

¹¹⁰ Koninklijk besluit van 19 mei 1959, nr. 128104, houdende wijziging in de taakverdeling, samenvoeging en naamswijziging van departementen.

Artikel 1 sub f van het subtaakbesluit Defensie Materieel Organisatie 2013 (hierna: subtaakbesluit) bepaalt dat JIVC onder Defensie Materieel Organisatie valt.

Artikel 7 van het subtaakbesluit kent de volgende taken toe aan de Directeur JIVC:

“Het Joint Informatievoorzieningscommando staat onder leiding van de Directeur JIVC die is belast met:

- a. Het met inachtneming van de aanwijzingen en richtlijnen van de Directeur Defensie Materieel Organisatie geven van ambtelijke leiding aan het JIVC;*
- b. Het met inachtneming van de regeling agentschappen van de Minister van Financiën invulling geven aan de rol van opdrachtgever voor het agentschap Operations voor het laten leveren van IV- en ICT-producten- en diensten;*
- c. Het leveren en instand houden van IV- ICT- en Informatiebeheer producten en diensten;*
- d. Het reguleren van vraag en aanbod om tot goede en betaalbare IV-voorzieningen te komen;*
- e. Het proactief zorgdragen voor innovatieve producten en diensten op IV-gebied;*
- f. Het zorgdragen voor voorspelbare kwaliteit, tijd en kosten van de geleverde diensten;*
- g. Het zorgdragen voor de doelmatige inrichting, de bedrijfsvoering en het interne beheer van het JIVC.”*

255

Op grond van het subtaakbesluit (in het bijzonder artikel 7 sub c en g) is het monitoren en loggen waarschijnlijk wel als taak van JIVC/DCSC te kwalificeren.

Toepassingsbereik AVG

Materieel toepassingsgebied

Bij het monitoren en loggen van het systeem worden persoonsgegevens verwerkt in de systemen van DCSC. Daarbij kan het gaan om alle categorieën persoonsgegevens. Dit komt omdat DCSC het hele systeem (alle datastromen) van Defensie monitort en logt. Als er een e-mail met daarin malware naar boven komt, dan kan in die e-mail in principe iedere categorie persoonsgegevens voorkomen.

Aangezien DCSC persoonsgegevens verwerkt valt deze activiteit op grond van artikel 2 AVG binnen het materieel toepassingsbereik van de AVG.

Territoriaal toepassingsgebied

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland valt de verwerking van persoonsgegevens van deze activiteit op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG.

Kortom, de AVG is van toepassing op deze activiteit die DCSC uitvoert.

Beoordeling activiteit

Artikel 5 AVG bepaalt aan welke beginselen de verwerking van persoonsgegevens moet voldoen. Deze beginselen worden hieronder nader uiteengezet in het licht van deze activiteit.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. DCSC heeft een DPIA uitgevoerd waarbij de grondslagen voor de verwerking zijn uitgewerkt. Hierna volgt een kopie van de tekst van de rechtmatigheid zoals DCSC deze heeft opgenomen in de DPIA. Daarna volgt onze beoordeling van de rechtmatigheid.

256

De volgende tekst is afkomstig uit de DPIA:

Gerechtvaardigd belang

“Het is een gerechtvaardigd belang van Defensie om de Defensie IT-infrastructuur te beschermen tegen cyberincidenten door interne controle en beveiliging en daarmee een bijdrage te leveren aan de digitale veiligheid en weerbaarheid.

Om het personeel van DCSC hun taak te kunnen laten uitvoeren binnen de kaders van de wet en regelgeving is in samenwerking met DJZ een juridisch kader DCSC opgesteld.¹¹¹

De belangen en de fundamentele vrijheden van de betrokkenen die tot bescherming van persoonsgegevens nopen, zijn daarbij goed afgewogen en wegen niet zwaarder dan de belangen van de verwerkingsverantwoordelijke.”

Algemeen belang

“Wet Beveiliging Netwerk- en Informatiesystemen (hierna: WBNI)

Met de WBNI is de EU-richtlijn 2016/1148 over netwerk- en informatiebeveiliging vanaf 9 november 2018 geïmplementeerd in de Nederlandse regelgeving. Hiermee komt er binnen de EU meer eenheid

¹¹¹ Juridisch Kader DCSC van 17 februari 2021.

in het beleid over netwerk- en informatiebeveiliging en wordt beoogd de (internationale) samenwerking te verbeteren, de digitale paraatheid te vergroten en de gevolgen van cyberincidenten te verkleinen.

Aanbieders van essentiële diensten (hierna: AED's) en digitale dienstverleners (hierna: DSP's) zijn op basis van de WBNl verplicht maatregelen te nemen om de kansen op en de gevolgen van incidenten te verkleinen. Ernstige incidenten moeten gemeld worden bij het Ministerie van Justitie & Veiligheid. Dit ministerie is aangewezen als het computer security incident response team (hierna: CSIRT) van Nederland.

Defensie heeft op grond van de WBNl geen verplichtingen, maar wel recht op:

- o *Bijstand van het Nationaal Cyber Security Centrum (hierna: NCSC) bij het nemen van maatregelen om de continuïteit van hun diensten te waarborgen of te herstellen;*
- o *Informatie en adviezen van het NCSC over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen.*

VIR/VIR BI2013

Op de beveiliging van bijzondere informatie zijn de bepalingen van het voorschrift VIRBI 2013 als aanvulling op het besluit voorschrift informatiebeveiliging rijksdienst 2007 en het BVR 2013 van toepassing.

257

Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen Rijksdienst"

Hierna volgt onze beoordeling van de rechtmatigheid.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens mogen verwerkt als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd. De taak moet daarnaast duidelijk en specifiek genoeg zijn omschreven zodat het voor de betrokkene duidelijk is dat er persoonsgegevens worden verwerkt en voor welk doel. Het is bovendien enkel toegestaan om de persoonsgegevens te verwerken die noodzakelijk zijn om die taak te vervullen. Artikel 7 sub c en g van het subtaakbesluit bepaalt dat JIVC is belast met het instant houden van IV en ICT beheer producten en diensten en dat JIVC zorg moet dragen voor de doelmatige inrichting, de bedrijfsvoering en het interne beheer van JIVC.

Wij zijn van mening dat uit deze taakomschrijving onvoldoende voorzienbaar is dat er persoonsgegevens kunnen worden verwerkt.

Daarnaast valt een subtaakbesluit niet als publieke taak te kwalificeren en is de taakomschrijving an sich onvoldoende specifiek omschreven, waardoor niet voorzienbaar is dat het noodzakelijk en evenredig is om persoonsgegevens te verwerken om de taak uit te voeren. Bovendien is het subtaakbesluit een ministeriële regeling, waardoor het – zelfs als op basis van de taakomschrijving voldoende voorzienbaar is dat er persoonsgegevens worden verwerkt – geen bevoegdheid kan scheppen in de zin van artikel 6 lid 1 sub e AVG. Om een dusdanige taak en bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een AOD, en in het verlengde daarvan een subtaakbesluit, missen deze rechtskracht.

Een publieke taak en bevoegdheid om in het kader van het algemeen belang persoonsgegevens te verwerken door middel van een scraper, al dan niet als bijvangst, ontbreekt. Dat de intentie niet is gericht op het verwerken van persoonsgegevens maakt deze conclusie niet anders.

Gerechtvaardigd belang

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak. In het geval dat het om een typisch bedrijfsmatige handeling voor een overheidsinstantie gaat is dit onder niet duidelijk gedefinieerde kaders wellicht een mogelijkheid. Daarnaast moet het verwerken van persoonsgegevens noodzakelijk en evenredig zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. Een voorbeeld van een typisch bedrijfsmatige handeling van overheidsinstanties is het beveiligen van overheidsgebouwen. Een dergelijke bedrijfsmatige handeling wijkt namelijk niet af van private organisaties die het gerechtvaardigd belang hebben hun eigendommen (waaronder panden) te beveiligen. Het is lastig om te beoordelen wat een typisch bedrijfsmatige handeling van een overheidsinstantie precies inhoudt. In de wet- en regelgeving, de literatuur en de rechtspraak is namelijk geen duidelijke definitie gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie. De activiteit die door DCSC wordt uitgevoerd is waarschijnlijk aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie, in dit geval van Defensie. Ingevolge overweging 49 AVG is de verwerking van persoonsgegevens voor zover strikt noodzakelijk en evenredig met het oog op netwerk- en informatiebeveiliging, aan te merken als een gerechtvaardigd belang van een overheidsinstantie.

De verwerking van persoonsgegevens bij deze activiteit is waarschijnlijk aan te merken als rechtmatig en noodzakelijk op grond van het gerechtvaardigd belang van Defensie om de interne IT-infrastructuur te beschermen. Het

beschermen van de IT-infrastructuur is ondersteunend aan – en helpt bij de verbetering van – de bedrijfsvoering van Defensie. Om vast te stellen of er sprake is van een gerechtvaardigd belang is het noodzakelijk om een belangenafweging te maken. Het is aan de verwerkingsverantwoordelijke om de afweging te maken of het verwerken van persoonsgegevens noodzakelijk en evenredig is en dat het gerechtvaardigd belang van Defensie prevaleert boven het belang van de betrokkene. Het gaat daarbij om een belangenafweging tussen het belang van de betrokkene en het belang van Defensie om de eigen IT-infrastructuur te beschermen.

Deze belangen zijn volgens ons onvoldoende afgewogen en uitgewerkt in de DPIA en het juridisch kader DCSC. Dat neemt niet weg dat activiteit 16a volgens ons waarschijnlijk wel voldoet aan het beginsel van rechtmatigheid, met de kanttekening dat een belangenafweging in de DPIA en/of het juridisch kader DCSC wordt ingevoegd. Concluderend wordt in beginsel op basis van de grondslag gerechtvaardigd belang voldaan aan het beginsel van rechtmatigheid.

Mogelijke knelpunten		Aanbevelingen
<i>Juridisch</i>		
1.	De grondslag om deze activiteit uit te voeren is niet (duidelijk genoeg) gedefinieerd als taak in de wet in het kader van de publieke taak voor het algemeen belang. Het juridisch kader is namelijk te algemeen om daar een specifieke taak uit te halen op grond waarvan DCSC persoonsgegevens mag verwerken. Daarom is deze activiteit ons inziens waarschijnlijk enkel op grond van het gerechtvaardigd belang uitvoerbaar. Er mist echter een vereiste belangenafweging tussen het belang van de betrokkenen en de belangen van Defensie.	Weeg de belangen van de betrokkenen af tegen de belangen van Defensie. Door deze belangenafweging te maken in de DPIA en het juridisch kader DCSC is de grondslag gerechtvaardigd belang conform artikel 6 lid 1 onder f AVG waarschijnlijk voldoende om activiteit 16a uit te voeren. DCSC spreekt de behoefte uit voor één cyberwet waar de bevoegdheden, rechten en plichten voor Defensie staan beschreven.
2.	DCSC ervaart privacy-issues met het verwerken van	Binnen Defensie bestaat de Regeling gedragsregels gebruik e-mail en

<p>persoonsgegevens van Defensiepersoneel van privéapparatuur aangemeld op het Defensienetwerk. Op het netwerk monitort DCSC alle datastromen. De hoofdtaak is het beschermen van het interne netwerk van Defensie. Af en toe detecteert DCSC 'gevaren', zoals malware op privé-apparatuur van Defensiepersoneel. De taak van DCSC is niet om deze apparaten te beschermen, maar heeft soms dus wel inzicht in mogelijke gevaren. DCSC mag in die gevallen niet optreden, terwijl dit wel makkelijk kan. Op het moment wordt in deze gevallen eerst toestemming gevraagd bij DJZ voordat actie wordt ondernomen.</p>	<p>internetvoorzieningen Defensie. Deze regeling geeft de wijze aan waarop bij Defensie en door Defensiepersoneel wordt omgegaan met de e-mail en internetvoorzieningen van Defensie. Ook wordt geregeld hoe en op welke wijze controle plaatsvindt. Conform artikel 2 van de regeling moet er een juiste balans bestaan tussen controle op verantwoord e-mail- en internetgebruik en de bescherming van privacy van werknemers. Uit de toelichting (algemeen) bij deze regeling blijkt dat de regeling niet toeziet op het gebruik door Defensiepersoneel van eigen privé-email en internetvoorziening. Op basis daarvan is het niet toegestaan om bijvoorbeeld malware op privé-apparatuur op te sporen.</p> <p>Een aanbeveling is het vergroten van de bewustwording bij Defensiepersoneel door middel van bijvoorbeeld phishingtests. Dit draagt bij aan de interne bescherming van het netwerk van Defensie, maar draagt er ook aan bij dat Defensiepersoneel zich beter weten te wapenen tegen eventuele phishingmails. Ons inziens wordt het mogelijke knelpunt hiermee (tenminste voor een gedeelte) gemitigeerd.</p>
--	---

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

Met betrekking tot het monitoren en loggen wordt er wel aan dit beginsel voldaan. Zo wordt het Defensiepersoneel op verschillende manieren geïnformeerd:

- *Via de Centrale Medezeggenschap Commissie (C-MC) Defensie wordt de informatie over het monitoren en loggen verspreid richting de decentrale MC's;*
- *Als een gebruiker inlogt op het Defensiesysteem dan krijgt hij/zij een melding dat al zijn/haar data wordt gelogd en wordt gebruikt voor monitoring ten behoeve van cybersecurity;*
- *Informatie verspreiding over de taakstelling van DCSC wordt gedaan middels de website/intranet;*
- *Informatie over de taakstelling van DCSC wordt tevens verspreid middels JICV nieuwsupdate of overige interne nieuwskanalen.*

Concluderend wordt bij deze activiteit voldaan aan het beginsel van behoorlijkheid en transparantie.

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigde doel worden verzameld. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

261

Het doel van deze activiteit is de digitale veiligheid- en weerbaarheid van Defensie waarborgen. Dit doel is welbepaald en uitdrukkelijk omschreven. De verwerking van persoonsgegevens vindt enkel plaats ten behoeve van dit doel. Na een beveiligingsincident verwijdert Defensie de persoonsgegevens weer volgens de geldende richtlijnen met betrekking tot bewaartermijnen. Er wordt dus voldaan aan het beginsel van doelbinding bij deze activiteit.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel worden verwerkt.

DCSC geeft bij deze activiteit invulling aan dataminimalisatie door enkel de persoonsgegevens te verwerken die relevant zijn voor de afhandeling van een incident. Zo wordt niet alle de metadata ingezien omdat deze niet altijd zijn gekoppeld aan een mogelijk cyberincident. Daarnaast vindt de verwerking enkel plaats aan de hand van bepaalde triggers. Zonder 'trigger' wordt het incident niet geregistreerd als zodanig en verwerkt DCSC geen persoonsgegevens. Mochten de verwerkte (persoons)gegevens naar aanleiding

van het incident uitwijzen dat er een (potentiële) strafrechtelijke overtreding is begaan dan wordt het incident (inclusief alle bijbehorende informatie) overgedragen aan de Koninklijke Marechaussee (hierna: KMar). Gelet op de aard van de activiteit zijn de verzamelde persoonsgegevens nodig om het doel te bereiken.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

De verwerkte persoonsgegevens bij incidenten zijn rechtstreeks afkomstig van de betrokkene. Defensie is verantwoordelijk, maar heeft geen invloed op de juistheid van de gegevens. Een actieve rol om persoonsgegevens te corrigeren ligt niet op de weg van Defensie gelet op de kern van deze activiteit. In beginsel wordt alsnog voldaan aan het beginsel van juistheid.

Opslagbeperking

Persoonsgegevens die worden verwerkt mogen op grond van artikel 5 lid 1 sub e AVG niet langer dan noodzakelijk is voor het doel van de verwerking worden bewaard. Op het moment dat de noodzakelijkheid om de gegevens te bewaren vervalt, dan moeten de gegevens worden gewist.

262

Op basis van de selectielijst van het Ministerie van Defensie hanteert DCSC verschillende bewaartermijnen.¹¹² Een ticket van een beveiligingsincident wordt vijf jaar bewaard, gegevens van defensiepassen zeven jaar (dit wordt in de toekomst tien jaar) en de bewaartermijn van het loggen is zes maanden. Uit het interview is naar voren gekomen dat DCSC deze bewaartermijnen naleeft. Er wordt dus voldaan aan het beginsel van opslagbeperking.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

Bij deze activiteit neemt DCSC het Defensiebeveiligingsbeleid (hierna: DBB) in acht. Daarom is er een goed beveiligingsniveau voor de persoonsgegevens die worden verwerkt. Ook gaat het om indirect herleidbare persoonsgegevens en

¹¹² Zie volgnummer 9.3.1 en 9.3.2 van de Selectielijst Ministerie van Defensie vanaf (1945) 2021, versie 2.1, pagina 69 -70.

gepseudonimiseerde persoonsgegevens. De persoonsgegevens worden op die manier beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Concluderend voldoet DCSC bij deze activiteit aan het beginsel van integriteit en vertrouwelijkheid.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG. De verwerkingsverantwoordelijke moet dit ook kunnen aantonen. Om dit aan te tonen moet de verantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden. Over de bouwstenen van het DCSC – waaronder het monitoren en loggen – voert het DCSC momenteel een DPIA uit. In de DPIA komen ook verschillende beginselen uit artikel 5 lid 1 AVG aan bod. Op basis van de DPIA voert DCSC ook mitigerende maatregelen uit. Momenteel vindt er een verwerking van persoonsgegevens plaats zonder dat deze is opgenomen in het verwerkingsregister. Volgens de respondent wordt de activiteit na het afronden van de DPIA opgenomen in het verwerkingsregister. Er is geen indicatie dat er (derde) verwerkers betrokken zijn bij deze activiteit. Het is dus niet nodig om de verplichtingen ook op te leggen aan een verwerker. Concluderend wordt voldaan aan de verantwoordingsplicht.

Mogelijk knelpunt

Naar aanleiding van de interviews is er een mogelijk knelpunt geïdentificeerd die niet per definitie toeziet op activiteit 14A of 14B. Dit algemene knelpunt ziet niet zo zeer op de beginselen van de AVG en heeft een algemene (ethische) strekking.

263

Mogelijke knelpunten		Aanbevelingen
<i>Ethisch</i>		
3.	Het JIVC kan niet doorlopend op basis van MSOB of militaire bijstand ondersteuning verlenen. De belangen, bijvoorbeeld het beschermen van (oud) Defensiepersoneel (Veteraneninstituut) tegen cybercrime, zijn helder. De capaciteit en kennis zijn eveneens aanwezig. Het is op dit moment niet mogelijk om extern deze capaciteit te leveren.	Beoordeel aan de voorkant of het wenselijk is dat JIVC (of een ander defensieonderdeel, bijvoorbeeld DCC) zich bezighouden met deze of soortgelijke activiteiten.

Conclusie

De activiteit kan in de huidige vorm doorgaan, maar er zijn mogelijk enkele knelpunten. Werk de (gerechtvaardigd) belangenafweging tussen het belang van de betrokkenen en de belangen van Defensie uit. De noodzakelijke belangenafweging ontbreekt volgens ons in de DPIA, daarom is niet met zekerheid te stellen of er sprake is van een gerechtvaardigd belang van Defensie om persoonsgegevens te verwerken, conform artikel 6 lid 1 sub f en overweging 49 AVG. Vanwege de aard van de aanbevelingen geven wij deze activiteit de kleur oranje.

Activiteit 14B

<zie vertrouwelijke bijlage>

Activiteit 15

<zie vertrouwelijke bijlage>

Activiteit 16

<zie vertrouwelijke bijlage>

Activiteit 17

<zie vertrouwelijke bijlage>

Activiteit 18

Omschrijving activiteit 18

Het Dienstcentrum Personeelslogistiek (hierna: DCPL) werft, selecteert en keurt nieuw militair- en burgerpersoneel voor Defensie. Jaarlijks worden ongeveer 4000-5000 mensen aangesteld. Aangezien slechts een klein deel van alle personen die zich aanmelden wordt aangesteld, moet DCPL door middel van campagnes een groot publiek bereiken. Het aanstellen van nieuw personeel gaat over verschillende schijven (werven, selecteren en keuren). Deze activiteit ziet toe op het onderdeel 'arbeidsmarktcommunicatie'.

Werven en Selecteren (hierna: WenS) omvat alle werving en selectie activiteiten, beginnend bij het opstellen van een wervingsstrategie en eindigend met de selectie van een kandidaat, inclusief vastlegging en bevestiging van arbeidsvoorwaarden. Het proces stopt bij 'klaar voor aanstelling'. Arbeidsmarktcommunicatie is op zichzelf gezien een onderdeel van werving en omvat arbeidsmarktcampagnes, sociale media en de website (www.werkenbij...).

Arbeidsmarktcommunicatie zit helemaal aan de voorkant van het WenS proces. Aan de hand van data gedreven campagnes wil DCPL zoveel mogelijk geschikte kandidaten interesseren voor een baan bij Defensie. Aan het begin van het proces (campagne voeren) richt DCPL zich tot een heel breed publiek. In deze fase verwerkt DCPL ook nog geen namen of andersoortige persoonsgegevens van mensen. Daar is DCPL ook nog niet in geïnteresseerd. Deze persoonsgegevens zijn pas relevant in de sollicitatiefase.

Arbeidsmarktcommunicatie ziet toe op de fase vóór het solliciteren. Alle stappen die daarna komen vallen daarom buiten de scope van deze activiteit. Defensie is actief op verschillende sociale mediakanalen. Dit is ook onderdeel van de arbeidsmarktcommunicatie. DCPL is actief op Facebook, Instagram, LinkedIn, YouTube en Twitter. Via de verschillende kanalen komen enorm veel vragen binnen van geïnteresseerden. Denk hierbij aan iemand die nog vragen heeft over een bepaalde functie of iemand die wil weten waar hij aan moet voldoen om in aanmerking te komen voor een functie. Ook plaatsen mensen verschillende opmerkingen via sociale mediakanalen. Denk bijvoorbeeld aan iemand die aangeeft dat hij die dag een keuring heeft voor Defensie. Om al deze vragen en opmerkingen goed te managen gebruikt DCPL het platform van Coosto. Via het platform van Coosto komen alle vragen en opmerkingen binnen en kunnen medewerkers eenvoudig reageren. Zo kan DCPL in een oogopslag alle sociale mediakanalen in de gaten houden en reageren op binnenkomende vragen. De reacties die DCPL geeft worden uit naam van Defensie gegeven en zijn openbaar. Zo kan iedereen de vragen en antwoorden zien. Het is ook een optie om via WhatsApp of e-mail contact op te nemen met

Defensie. Via deze weg stuurt DCPL antwoorden op vragen die ze in verband met de vertrouwelijkheid beter niet openbaar kunnen sturen. Ook merkt DCPL dat jongeren tegenwoordig liever via WhatsApp communiceren dan bijvoorbeeld via de telefoon. Als het voor jongeren alleen mogelijk is om telefonisch contact op te nemen, dan zijn het toch vaak de ouders die bellen. Dit wil DCPL voorkomen, omdat ze de geïnteresseerden zelf willen spreken. Op het proces van WenS is een Data Protection Impact Assessment (hierna: DPIA) uitgevoerd.¹¹³ Op basis daarvan zijn mitigerende maatregelen genomen, zoals het beter beschermen van de systemen, het sluiten van verwerkersovereenkomst(en) en het stellen van extra eisen aan de betrokken personen in het proces. Deze personen moeten bijvoorbeeld een eed afleggen en er wordt een veiligheidsonderzoek uitgevoerd.

Bij het proces van arbeidsmarktcommunicatie is DCPL niet geïnteresseerd in namen of soortgelijke persoonsgegevens. Deze persoonsgegevens komen pas aan bod op het moment dat een geïnteresseerde solliciteert. Als geïnteresseerden directe vragen stellen is het niet te voorkomen om persoonsgegevens te verwerken. Daarbij kunnen de voor- en achternaam en IP-adressen van betrokkenen worden verwerkt. Slechts enkele collega's hebben toegang tot die IP-adressen, omdat dit noodzakelijk is om het systeem te onderhouden. Dit wordt voornamelijk vanuit veiligheidsoogpunt gedaan. Het is namelijk mogelijk dat er een veiligheidsonderzoek (bijvoorbeeld na een incident, zoals onbevoegde toegang of een hack) plaatsvindt. Als dat het geval is dan wil DCPL de mogelijkheid hebben om nog bij deze gegevens te kunnen. Tot op heden is er geen dergelijk veiligheidsonderzoek verricht.

270

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DCPL, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 44 Grondwet (hierna: Gw) bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministeries staan onder leiding van een minister. Bij koninklijk besluit is het Ministerie van Defensie ingesteld.¹¹⁴

¹¹³ Gegevensbeschermingseffectbeoordeling Rijksbrede Werving en Selectie (hierna: DPIA WenS).

¹¹⁴ Koninklijk besluit van 19 mei 1959, nr. 128104, houdende wijziging in de taakverdeling, samenvoeging en naamswijziging van departementen.

Artikel 1 sub f van het AOD bepaalt dat het Ministerie van Defensie de Directeur Communicatie als verantwoordelijke kent.

Artikel 7 AOD bepaalt het volgende:

“De Directeur Communicatie is belast met:

- a. Het met inachtneming van de aanwijzingen van de Secretaris-Generaal geven van ambtelijke leiding aan de Directie Communicatie;*
- b. De woordvoering namens de politieke, ambtelijke en militaire leiding, voor zover het de verantwoordelijkheid van de Minister van Defensie betreft;*
- c. Het gevraagd en ongevraagd adviseren van de politieke, ambtelijke en militaire leiding inzake mediagevoelige aangelegenheden;*
- d. De externe, interne en arbeidsmarktcommunicatie;*
- e. Het ontwikkelen, coördineren en handhaven van integraal en uitvoerend communicatiebeleid in afstemming met de Directeur-Generaal Beleid en de Rijksvoorlichtingsdienst.”*

Naast dat Directie Communicatie (hierna: DCO) verantwoordelijk is voor arbeidsmarktcommunicatie bepaalt artikel 1 sub o van het AOD dat het Ministerie van Defensie de Commandant Defensie Ondersteuningscommando als verantwoordelijke kent voor P&O aangelegenheden.

271

Meer specifiek bepaalt artikel 16 AOD over de Commandant Defensie Ondersteuningscommando het volgende:

“De Commandant Defensie Ondersteuningscommando is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van ambtelijke leiding aan het Defensie Ondersteuningscommando;*
- b. het binnen de kaders wereldwijd en zo veel mogelijk geïntegreerd leveren van producten en diensten op de terreinen huisvesting, beveiliging, facilitaire diensten, transport, catering, P&O dienstverlening, gezondheidszorg en opleidingen aan alle Defensieonderdelen en het waarborgen van de kwaliteit van de dienstverlening op die gebieden;*
- c. het verzorgen van rijksbreed categoriemanagement voor de aan Defensie toegewezen categorieën die bij het Defensie Ondersteuningscommando zijn belegd;*
- d. infrastructuurprojecten binnen de kaders van het defensiematerieelproces (DMP);*
- e. de advisering op de toegewezen functiegebieden en het van daaruit ondersteunen van de overige defensieonderdelen.”*

Subtaakbesluit

Artikel 26 AOD bepaalt dat de Commandant Defensie Ondersteuningscommando op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Dienstencentra 2012

Het Commando DienstenCentra (hierna: CDC) is de voorloper van de huidige Defensie Ondersteuningscommando (hierna: DOSCO) waar DCPL onder valt. Er is geen subtaakbesluit gevonden aangaande DOSCO en/of DCPL. Vanwege deze omstandigheid is aansluiting gezocht en gevonden bij het subtaakbesluit CDC 2012 (hierna: subtaakbesluit) en de bijbehorende (zoveel mogelijk overeenkomende) terminologie.¹¹⁵

Artikel 1 sub f subtaakbesluit bepaalt dat het Commando Dienstencentra bestaat uit de Divisie Personeel & Gezondheid. Artikel 4 van het subtaakbesluit kent de volgende taken toe aan de commandant van de Divisie Personeel en Gezondheid:

"De Divisie Personeel & Gezondheid staat onder leiding van de Commandant van de Divisie Personeel & Gezondheid die is belast met:

- a. het met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Commando DienstenCentra geven van ambtelijke leiding aan de Divisie Personeel & Gezondheid;*
- b. het ten behoeve van de defensieonderdelen realiseren van de instroom van militair personeel;*
- c. het, in de meest brede zin, leveren van de volgende diensten: medische keuringen, psychologische selecties en adviezen, juridische diensten, gedragswetenschappelijk onderzoek, en specialistisch advies en ondersteuning op het gebied van personeel en organisatie, en formatie;*
- d. het bieden van bedrijfsmaatschappelijke hulp- en dienstverlening aan personeel, thuisfront en organisatie;*
- e. het creëren van de bedrijfsvoeringtechnische voorwaarden waaronder de door de HDP opgedragen uitvoering van taken op het gebied van defensiebrede re-integratie- en externe bemiddeling van defensiepersoneel door respectievelijk het DienstenCentrum Re-integratie en het DienstenCentrum Externe Bemiddeling Defensiepersoneel kunnen worden uitgevoerd;*
- f. het onafhankelijke expertisecentrum voor integriteit met als taak het terugdringen van ongewenst gedrag. De Centrale Organisatie Integriteit*

¹¹⁵ Subtaakbesluit Commando DienstenCentra 2012.

Defensie (COID) ondersteunt commandanten bij de uitvoering van het integriteitbeleid met adviezen, voorlichting, trainingen morele oordeelsvorming, risicoanalyses en onderzoeken. COID heeft een centraal meldpunt voor ongewenst gedrag en adviseert de defensieorganisatie en de medewerkers over integriteit en de Wet bescherming persoonsgegevens;

- g. de verantwoordelijkheid voor de bedrijfsvoering van de Divisie Personeel & Gezondheid;*
- h. het fungeren als aanspreekpunt van de Divisie Personeel & Gezondheid voor klanten en opdrachtgevers;*
- i. het in overleg met de klant c.q. opdrachtgever vaststellen van de leveringsvoorwaarden van producten en diensten van de Divisie Personeel & Gezondheid binnen de randvoorwaarden van de Commandant Commando DienstenCentra en de Bestuursstaf;*
- j. het mede begeleiden van relevant onderzoek in het kader van de Strategische kennis- en*
- k. innovatieagenda (SKIA) en het mede waarborgen van de kwaliteit, tijdigheid, bruikbaarheid en defensiebrede beschikbaarheid van kennisproducten conform de eisen die zijn gesteld door en in afstemming met de desbetreffende beleidsverantwoordelijken;*
- l. de informatievoorziening ten behoeve van de Commandant Commando DienstenCentra, gegeven het eigen terrein van verantwoordelijkheid;*
- m. het leveren van: 1. medisch specialistische zorg, revalidatiezorg en geestelijke gezondheidszorg; 2. zorgcapaciteit (medisch specialistische en revalidatie) voor de opvang van (grotere aantallen) militaire en civiele slachtoffers; 3. militair geneeskundige opleidingen; 4. geneeskundige goederen, geneesmiddelen, geneeskundige uitrustingen, assemblage en diensten; 5. bloed en bloedproducten; 6. uitzendbaar medisch specialistisch personeel; 7. preventie en/of tijdige interventie op arbeidsrisico's, verzuimbegeleiding en (vroeg) reïntegratieactiviteiten om de inzetbaarheid van personeel te bevorderen en te behouden; 8. geneeskundige adviezen inzake de functie- c.q. dienstgeschiktheid van burgerambtenaren en militairen."*

273

Op grond van het subtaakbesluit (in het bijzonder artikel 4 sub b) is de arbeidsmarktcommunicatie te kwalificeren als taak van DCPL.

Toepassingsbereik AVG

Materieel toepassingsbereik

Bij deze activiteit horen de volgende verwerkingen:

- Beantwoorden van vragen gesteld via sociale media via het platform van Coosto;

- Beantwoorden van vragen die binnen komen via de website en e-mail van Defensie.
- Buiten arbeidsmarktcommunicatie om, maar vloeit hier uit voort:
Verzamelen IP-adres ten behoeve van potentiële veiligheidsrisico's.

Aangezien er persoonsgegevens worden verwerkt valt deze activiteit op grond van artikel 2 AVG binnen het materieel toepassingsbereik van de AVG.

Territoriaal toepassingsbereik

De verwerkingen vallend onder deze activiteit richten zich op Nederlanders en vinden plaats in Nederland. Dit doet zich voor onder de verantwoordelijkheid van de Minister van Defensie, waardoor het binnen het territoriaal toepassingsbereik van de AVG valt.

Kortom, de AVG is van toepassing op deze activiteit.

Beoordeling activiteit

In deze paragraaf wordt de activiteit getoetst aan de beginselen voor het verwerken van persoonsgegevens uit artikel 5 AVG.

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. We beperken ons in deze beoordeling tot de meest voor de hand liggende grondslagen.

Toestemming

Artikel 6 lid 1 sub a AVG bepaalt dat persoonsgegevens verwerkt mogen worden als een betrokkene hiervoor ondubbelzinnig toestemming geeft. De respondenten hebben aangegeven dat het stellen van vragen en de daaronder vallende verwerking van persoonsgegevens via de website werkenbijdefensie.nl is gebaseerd op de grondslag toestemming. Mogelijk wordt de betrokkene hierover onvoldoende geïnformeerd en is sprake van het volgende knelpunt:

Mogelijk knelpunt		Aanbeveling
<i>Juridisch (grondslag toestemming)</i>		
1	Het is ons opgevallen dat er geen ondubbelzinnige, actieve handeling vooraf gaat aan het stellen van een vraag via	Zorg dat de betrokkene wordt geïnformeerd over de verwerking. Het eisen van een actieve handeling van de betrokkene kan hiervoor een

https://werkenbijdefensie.nl/contact/stuur-een-mail . Hierdoor is het voor de betrokkene mogelijk onvoldoende duidelijk welke persoonsgegevens voor welk doel worden verwerkt. Dit heeft mogelijk tot consequentie dat er meer persoonsgegevens worden gedeeld en verwerkt dan strikt noodzakelijk voor deze verwerking.	invulling zijn, bijvoorbeeld het aanvinken van een akkoordverklaring. Voor een voorbeeld wijzen wij naar: https://www.rijksoverheid.nl/contact/informatie-rijksoverheid/e-mail-sturen Als dit proces goed wordt ingericht is het voor het stellen van vragen mogelijk om een beroep te doen op de grondslag toestemming.
--	--

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens mogen worden verwerkt als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd waarbij het voor de betrokkene duidelijk moet zijn dat er persoonsgegevens worden verwerkt. Bovendien is het alleen toegestaan om persoonsgegevens op basis van deze grondslag te verwerken als het noodzakelijk is voor de vervulling van de publieke taak.

275

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens mogen worden verwerkt als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd. De taak moet daarnaast duidelijk en specifiek genoeg zijn omschreven dat het voor de betrokkene helder is dat er persoonsgegevens worden verwerkt en voor welk doel. Het is bovendien enkel toegestaan om de persoonsgegevens te verwerken die noodzakelijk zijn om die taak te vervullen. Een subtaakbesluit is niet als publieke taak te kwalificeren en de taakomschrijving is op zichzelf onvoldoende specifiek omschreven, waardoor niet voorzienbaar is dat het noodzakelijk en evenredig is om persoonsgegevens te verwerken om de taak uit te voeren. Bovendien is het subtaakbesluit een ministeriële regeling, waardoor het – zelfs als op basis van de taakomschrijving voldoende voorzienbaar is dat er persoonsgegevens worden verwerkt – geen bevoegdheid kan scheppen in de zin van artikel 6 lid 1 sub e AVG. Om een dussdanige taak en bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een AOD, en in het verlengde daarvan een subtaakbesluit, missen deze rechtskracht.

In dit geval kan DCPL geen beroep doen op de verwerkingsgrondslag algemeen belang voor de uitvoering van deze activiteit. Om een bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een subtaakbesluit mist deze rechtskracht.

Gerechtvaardigd belang Coosto

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak. In het geval dat het om een typisch bedrijfsmatige handeling voor een overheidsinstantie gaat is dit onder niet duidelijk gedefinieerde kaders wellicht een mogelijkheid. Daarnaast moet het verwerken van persoonsgegevens noodzakelijk zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. Een voorbeeld van een typisch bedrijfsmatige handeling van overheidsinstanties is het beveiligen van overheidsgebouwen. Een dergelijke bedrijfsmatige handeling wijkt namelijk niet af van private organisaties die het gerechtvaardigd belang hebben hun eigendommen (waaronder panden) te beveiligen. Het is lastig om te beoordelen wat een typisch bedrijfsmatige handeling van een overheidsinstantie precies inhoudt. In de wet- en regelgeving, de literatuur en de rechtspraak is namelijk geen duidelijke definitie gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie.

276

De grondslag die van toepassing is op de persoonsgegevens die via het platform van Coosto worden verwerkt is waarschijnlijk het gerechtvaardigd belang conform artikel 6 lid 1 sub f AVG. Het belang van Defensie is bij deze activiteit gelegen in het verhogen van de efficiëntie bij het beantwoorden van vragen die via de verschillende kanalen binnenkomen. Het beantwoorden van (algemene) vragen via de verschillende kanalen wijkt volgens ons niet af van private organisaties en is daarmee waarschijnlijk aan te merken als een typisch bedrijfsmatige handeling van een overheidsinstantie. Via Coosto is het mogelijk om vragen en opmerkingen die via verschillende sociale media kanalen binnenkomen op een centrale plek te verzamelen en te beantwoorden. Dit maakt het mogelijk om gelet op de hoeveelheid vragen en platforms efficiënt te werk te gaan.

Bij deze activiteit wordt dus voor wat betreft het gebruik van Coosto voldaan aan het beginsel van rechtmatigheid. Het is echter wel van belang dat de belangen van Defensie worden afgewogen tegen de belangen van de betrokkene, waarbij de noodzakelijkheid en evenredigheid in het bijzonder moeten worden getoetst.

Behoorlijkheid en transparantie

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG behoorlijk en transparant zijn. Dit houdt in dat het voor de betrokkene duidelijk moet zijn dat er van hem of haar persoonsgegevens worden verzameld, gebruikt, geraadpleegd of op een andere manier worden verwerkt. Daarnaast moet het voor de betrokkene duidelijk zijn wie de verantwoordelijke is voor de verwerking van persoonsgegevens en wat daarvan het doel is.

In de privacyverklaring op de website werkenbijdefensie.nl/privacyverklaring staat welke persoonsgegevens Defensie verwerkt en wat hiervan de doelen zijn. Hiermee voldoet DCPL/Defensie aan het beginsel van behoorlijkheid en transparantie. Wel zijn er mogelijk knelpunten:

Mogelijk knelpunten		Aanbevelingen
Juridisch (privacyverklaring + verwerking buiten EER)		
2.	De privacyverklaring op de website werkenbijdefensie.nl/privacyverklaring schiet mogelijk op enkele vlakken tekort: Verwerking van persoonsgegevens in Coosto als derde partij wordt niet genoemd. De bijbehorende grondslag hiervoor is daarom ook niet uitgewerkt; Er is niets opgenomen over geautomatiseerde besluitvorming, terwijl hier wel gebruik van wordt gemaakt. Denk hierbij aan de uitsluiting op basis van leeftijd of nationaliteit. Een 'afwijzing' vindt dan geautomatiseerd plaats.	De privacyverklaring is voor het laatst gewijzigd op 1 mei 2020. Het is raadzaam om een proces in te richten waarbij bijvoorbeeld jaarlijks de privacyverklaring wordt bekeken en zo nodig geüpdatet. Neem in ieder geval Coosto en geautomatiseerde besluitvorming op in de volgende versie.
3.	Het is vrijwel onvermijdelijk om bij arbeidscommunicatie geen gebruik te maken van de big tech firma's voor effectieve campagnevoering. Hierdoor vindt er data doorgifte naar de Verenigde Staten en mogelijk andere landen buiten de Europese Economische Ruimte (hierna: EER) plaats. Het probleem hierbij is dat het niet mogelijk is om individuele afspraken	Betrokkenen die gebruikmaken van sociale media en WhatsApp zijn reeds zelfstandig akkoord gegaan met de verwerking van persoonsgegevens buiten de EER. Het is wel aan te raden om dit in het kader van transparantie ook in de privacyverklaring van werkenbijdefensie.nl op te nemen. Geef daarbij ook een toelichting dat er sprake is van internationale doorgifte van

<p>te maken met deze partijen. Het is namelijk alleen mogelijk om van deze platformen gebruik te maken op het moment dat de gebruikersvoorwaarden worden geaccepteerd. Aangezien jongeren veel gebruik maken van sociale media en WhatsApp is het wel noodzakelijk om jongeren op deze manier te bereiken. DCPL verwijderd gesprekken via WhatsApp naderhand ook. Het is onduidelijk of dit dan ook aan de andere kant, bij WhatsApp/Meta, gebeurt. Andere opties – zoals Signal - worden niet als wenselijk gezien omdat daar te weinig mensen gebruik van maken.</p>	<p>persoonsgegevens en geef aan wat daarvan de gevolgen zijn.</p> <p>Het is verstandig om een heldere standaardtekst op te stellen om te versturen zodra een betrokkene contact zoekt via WhatsApp. Plaats deze tekst ook op in de privacyverklaring van Contact - WerkenbijDefensie.nl.</p>
--	--

Doelbinding

Artikel 5 lid 1 sub b AVG stelt dat iedere verwerking van persoonsgegevens altijd voor een helder, vooraf en uitdrukkelijk omschreven en gerechtvaardigd doel moet worden verwerkt. Het is niet toegestaan om persoonsgegevens vervolgens verder te verwerken voor een doel dat zich niet verenigt met het oorspronkelijke doel.

278

De doelen zijn voldoende duidelijk omschreven in de privacyverklaring. Persoonsgegevens worden alleen voor de beschreven doelen verwerkt. Wij hebben geen indicatie dat de persoonsgegevens verder worden verwerkt voor andere doeleinden. Er wordt aan het beginsel van doelbinding voldaan.

Minimale gegevensverwerking

Volgens artikel 5 lid 1 sub c AVG mogen niet meer persoonsgegevens worden verwerkt dan noodzakelijk is om het doel te bereiken. Dit houdt in dat er niet te veel en ook niet te weinig gegevens over de betrokkene voor het te bereiken doel mogen worden verwerkt. Bij het beantwoorden van vragen worden alleen persoonsgegevens verwerkt die strikt noodzakelijk zijn om de vragen te beantwoorden. Verder is er geen indicatie dat er meer persoonsgegevens worden verwerkt dan noodzakelijk is.

Privacy by default

Bij het stellen van een vraag via de website wordt gebruikgemaakt van vrije invulvelden. Het risico bestaat dat een betrokkene in deze velden gevoelige en/of bijzondere persoonsgegevens invult. Wij raden aan om een extra

opmerking toe te voegen om de betrokkene erop te wijzen zo min mogelijk persoonsgegevens in te vullen. Zo wordt mogelijk voorkomen dat er meer persoonsgegevens worden verwerkt dan strikt noodzakelijk is.

Juistheid

Artikel 5 lid 1 sub d AVG bepaalt dat de verwerkingsverantwoordelijke ervoor moet zorgen dat de gegevens correct en actueel zijn. Gevolg hiervan is dat de verantwoordelijke gegevens die niet meer actueel zijn moet corrigeren of wissen.

Kandidaten vullen de gegevens zelf in. De vragen die worden gesteld via sociale media en binnenkomen via Coosto zijn rechtstreeks afkomstig van de betrokkene. Er is dus geen (rechtstreekse) invloed uit te oefenen op de juistheid van de persoonsgegevens. Uiteraard kan het voorkomen dat de persoonsgegevens niet juist zijn, bijvoorbeeld doordat er een foutieve naam is ingevuld of een betrokkene een typefout maakt. De verwerkingsverantwoordelijke blijft overigens wel altijd verantwoordelijk voor de juistheid van de gegevens. Er is echter een proces ingericht voor betrokkenen om inzage te verlenen en (op verzoek of indien nodig) te rectificeren.¹¹⁶ Er wordt bij deze activiteit voldaan aan het beginsel van juistheid.

279

Opslagbeperking

Persoonsgegevens mogen op grond van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan strikt noodzakelijk is voor het doel van de verwerking. Op het moment dat de noodzakelijkheid om de persoonsgegevens te bewaren vervalst, dan moeten de persoonsgegevens worden gewist.

Uit de selectielijst van het Ministerie van Defensie blijkt dat het verwerken van persoonsgegevens in het kader van werving zowel intern als extern kan plaatsvinden. Onder werving wordt verstaan; het verzamelen en beheren van vacaturegegevens, interne/externe vacaturepublicaties en het onder de aandacht brengen van vacatures bij belangstellenden tijdens informatie- en kennismakingsdagen en banenwinkels. Deze gegevens worden bewaard voor een periode van vijf jaren.¹¹⁷

Gegevens over potentiële kandidaten (het kandidaatprofiel) worden ingevolge de DPIA WenS voor de periode van één jaar bewaard. Daarmee wordt aan het beginsel van opslagbeperking voldaan.

¹¹⁶ Privacyrechten persoonsgegevens, Ministerie van Defensie,

<https://www.defensie.nl/onderwerpen/privacyrechten/privacyrechten-persoonsgegevens>.

¹¹⁷ Zie volgnummer 9.1.1 van de Selectielijst Ministerie van Defensie vanaf (1945) 2021, versie 2.1, pagina 56.

Integriteit en vertrouwelijkheid

Op grond van artikel 5 lid 1 sub f AVG moet de verwerkingsverantwoordelijke maatregelen nemen om de verwerkte persoonsgegevens te beschermen tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

DCPL neemt het Defensie Beveiligingsbeleid (hierna: DBB) bij deze activiteit in acht. Daarom is er een goed beveiligingsniveau van de persoonsgegevens die worden verwerkt. De persoonsgegevens worden op die manier beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging. Daarmee wordt aan het beginsel van integriteit en vertrouwelijkheid voldaan.

Verantwoordingsplicht

Uit artikel 5 lid 2 AVG volgt dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de beginselen van artikel 5 lid 1 AVG en dit moet kunnen aantonen. Om dit aan te tonen moet de verwerkingsverantwoordelijke onder andere een register van verwerkingsactiviteiten bijhouden.

DCPL voldoet aan dit beginsel, omdat deze activiteit is opgenomen in het verwerkingsregister.¹¹⁸ Ook is met Coosto een verwerkersovereenkomst gesloten en is er een DPIA uitgevoerd over het proces van WenS.

280

Conclusie

Deze activiteit is als onderdeel van WenS onderzocht door middel van een rijksbrede DPIA. Ondanks deze DPIA en de daarin voorgestelde mitigerende maatregelen zijn er specifiek gericht op arbeidsmarktcommunicatie enkele mogelijke knelpunten gesignaleerd. Deze blokkeren de doorgang van deze activiteit in de huidige vorm echter niet. Wel zijn er met betrekking tot de mogelijke knelpunten aanbevelingen opgenomen. Daarom krijgt deze activiteit de kleur groen.

¹¹⁸ Werving en selectie (WenS) | avgregisterrijksoverheid.nl

Activiteit 19

Omschrijving activiteit 19

Bureau accountmanagement, onderdeel van het Dienstcentrum Personeelslogistiek (hierna: DCPL) voert arbeidsmarktanalyses uit. De arbeidsmarktanalist gebruikt hiervoor (geaggregeerde) data uit verschillende bronnen. Het doel van een arbeidsmarktanalyse is het creëren van een duidelijk beeld van de ontwikkelingen op de arbeidsmarkt. Door de knelpunten op de arbeidsmarkt te analyseren constateert de arbeidsmarktanalist waar de krapte zit. Hier kan DCPL dan tijdig op reageren. Volgens de respondenten is de aangeleverde geaggregeerde informatie aan de voorkant geanonimiseerd en door Defensie niet te herleiden naar natuurlijke personen.

Daarnaast voert de arbeidsmarktanalist doelgroeponderzoeken uit. Dit zijn bijvoorbeeld rondetafelgesprekken met een aantal jongeren om te praten over wat ze belangrijk vinden bij een werkgever. Hier probeert Defensie aansluiting bij te vinden. Ook test en analyseert de arbeidsmarktanalist campagnes bij verschillende doelgroepen om te onderzoeken of de informatie zoals getoond voldoende is.

Voor het opstellen van arbeidsmarktanalyses gebruikt de arbeidsmarktanalist aangeleverde informatie uit de volgende bronnen:

- *Centraal Plan Bureau, Centraal Bureau voor de Statistiek en Eurostat*
Het Centraal Plan Bureau (hierna: CPB), het Centraal Bureau voor de Statistiek (hierna: CBS) en Eurostat (op Europees niveau) leveren geanonimiseerde, publiek toegankelijke gegevens. Hierdoor kan de arbeidsmarktanalist inzoomen op bepaalde onderdelen in de arbeidsmarkt of op bepaalde opleidingen. Bijvoorbeeld hoeveel vliegtuigonderhoudstechnici er jaarlijks afstuderen of hoeveel vrouwen er een technische opleiding volgen. Door deze informatie weet DCPL wat de maximale grootte is van de te benaderen groep.
- *Dienst Uitvoering Onderwijs*
Van Dienst Uitvoering Onderwijs (hierna: DUO) wordt informatie verzameld over hoeveel mensen er afstuderen en in welke studierichting.
- *MBO-raad en HBO-raad*
Defensie participeert in de opleiding Veiligheid & Vakmanschap (hierna: VeVa). Dit is een mbo-opleiding waarvoor Defensie instructeurs levert. De MBO-raad voert arbeidsmarktanalyses uit, onder andere voor Werken in Nederland ten behoeve van het inzichtelijk maken van arbeidsmarktperspectieven. Voor Defensie is het uiteraard interessant om

zoveel mogelijk mensen te werven die de VeVa-opleiding volgen. Het is niet verplicht om in dienst te gaan bij Defensie na voltooiing van deze opleiding. Het doel is namelijk het behalen van een diploma. De sollicitatie voor een baan bij Defensie vindt pas plaats na het behalen van een diploma. Daarbij doorlopen geïnteresseerden dezelfde stappen als andere sollicitanten (onder andere keuringen).

De HBO-raad levert in hoofdlijnen soortgelijke informatie aan bij Defensie. Deze informatie ziet dan uiteraard toe op hbo-studenten in plaats van mbo-studenten.

- *Samenwerkingsverband Beroepsonderwijs*
Samenwerkingsverband Beroepsonderwijs (hierna: SBB) is een brancheorganisatie die in de gaten houdt wat de arbeidsmarktperspectieven zijn van studenten met een praktijkopleiding. Door middel van deze informatie krijgt Defensie inzicht in hoeveel mensen een bepaalde (praktische) opleidingen volgen.
- *Intelligence Group*
Intelligence Group is een onderzoeksbureau op de arbeidsmarkt dat met panels, metadata en/of met organisaties zoals CPB en DUO (samen)werkt. Intelligence Group heeft samen met Jobfeed een tool ontwikkeld. Met deze tool brengen ze de schaarste op de arbeidsmarkt in verschillende leeftijdscategorieën in kaart. Intelligence Group maakt ook het gebruik van sociale media op hoofdlijnen inzichtelijk. Dit gaat om allemaal strikt geanonimiseerde data, verzameld vanuit publieke bronnen en ontsloten door web based interfaces.
- *Uitvoeringsorganisatie Bedrijfsvoering Rijk*
Uitvoeringsorganisatie Bedrijfsvoering Rijk (hierna: UBR) levert advies en informatie over banen binnen de sector Rijk.
- *Centrum Arbeidsverhoudingen Overheidspersoneel*
Centrum Arbeidsverhoudingen Overheidspersoneel (hierna: CAOP) pleegt centraal overleg voor overheidspersoneel. De organisatie verzamelt algemene trends. Defensie geeft CAOP bepaalde klussen om uit te voeren. Dit ziet niet altijd toe op werving en selectie.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DCPL, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het

Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 44 Grondwet (hierna: Gw) bepaalt dat bij koninklijk besluit ministeries worden ingesteld. Deze ministeries staan onder leiding van een minister. Bij koninklijk besluit is het Ministerie van Defensie ingesteld.¹¹⁹

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub o van het AOD bepaalt dat het Ministerie van Defensie de Commandant Defensie Ondersteuningscommando als verantwoordelijke kent.

Artikel 16 AOD bepaalt over de Commandant Defensie Ondersteuningscommando het volgende:

"De Commandant Defensie Ondersteuningscommando is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van ambtelijke leiding aan het Defensie Ondersteuningscommando;*
- b. het binnen de kaders wereldwijd en zo veel mogelijk geïntegreerd leveren van producten en diensten op de terreinen huisvesting, beveiliging, facilitaire diensten, transport, catering, P&O dienstverlening, gezondheidszorg en opleidingen aan alle Defensieonderdelen en het waarborgen van de kwaliteit van de dienstverlening op die gebieden;*
- c. het verzorgen van rijksbreed categoriemanagement voor de aan Defensie toegewezen categorieën die bij het Defensie Ondersteuningscommando zijn belegd;*
- d. infrastructuurprojecten binnen de kaders van het defensiematerieelproces (DMP);*
- e. de advisering op de toegewezen functiegebieden en het van daaruit ondersteunen van de overige defensieonderdelen."*

283

Subtaakbesluit

Artikel 26 AOD bepaalt dat de Commandant Defensie Ondersteuningscommando op basis van het Algemeen organisatiebesluit Defensie 2021 een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Dienstencentra 2012

Het Commando DienstenCentra (hierna: CDC) is de voorloper van de huidige Defensie Ondersteuningscommando (hierna: DOSCO) waar DCPL onder valt. Er is geen subtaakbesluit gevonden aangaande DOSCO en/of DCPL. Vanwege

¹¹⁹ Koninklijk besluit van 19 mei 1959, nr. 128104, houdende wijziging in de taakverdeling, samenvoeging en naamswijziging van departementen.

deze omstandigheid is aansluiting gezocht en gevonden bij het subtaakbesluit CDC 2012 (hierna: subtaakbesluit) en de bijbehorende (zoveel mogelijk overeenkomende) terminologie.¹²⁰

Artikel 1 sub f subtaakbesluit bepaalt dat het Commando Dienstencentra bestaat uit de Divisie Personeel & Gezondheid. Artikel 4 van het subtaakbesluit kent de volgende taken toe aan de commandant van de Divisie Personeel en Gezondheid:

“De Divisie Personeel & Gezondheid staat onder leiding van de Commandant van de Divisie Personeel & Gezondheid die is belast met:

- a. het met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Commando DienstenCentra geven van ambtelijke leiding aan de Divisie Personeel & Gezondheid;*
- b. het ten behoeve van de defensieonderdelen realiseren van de instroom van militair personeel;*
- c. het, in de meest brede zin, leveren van de volgende diensten: medische keuringen, psychologische selecties en adviezen, juridische diensten, gedragswetenschappelijk onderzoek, en specialistisch advies en ondersteuning op het gebied van personeel en organisatie, en formatie;*
- d. het bieden van bedrijfsmaatschappelijke hulp- en dienstverlening aan personeel, thuisfront en organisatie;*
- e. het creëren van de bedrijfsvoeringtechnische voorwaarden waaronder de door de HDP opgedragen uitvoering van taken op het gebied van defensiebrede re-integratie- en externe bemiddeling van defensiepersoneel door respectievelijk het DienstenCentrum Re-integratie en het DienstenCentrum Externe Bemiddeling Defensiepersoneel kunnen worden uitgevoerd;*
- f. het onafhankelijke expertisecentrum voor integriteit met als taak het terugdringen van ongewenst gedrag. De Centrale Organisatie Integriteit Defensie (COID) ondersteunt commandanten bij de uitvoering van het integriteitbeleid met adviezen, voorlichting, trainingen morele oordeelsvorming, risicoanalyses en onderzoeken. COID heeft een centraal meldpunt voor ongewenst gedrag en adviseert de defensieorganisatie en de medewerkers over integriteit en de Wet bescherming persoonsgegevens;*
- g. de verantwoordelijkheid voor de bedrijfsvoering van de Divisie Personeel & Gezondheid;*
- h. het fungeren als aanspreekpunt van de Divisie Personeel & Gezondheid voor klanten en opdrachtgevers;*

¹²⁰ Subtaakbesluit Commando DienstenCentra 2012.

- i. *het in overleg met de klant c.q. opdrachtgever vaststellen van de leveringsvoorwaarden van producten en diensten van de Divisie Personeel & Gezondheid binnen de randvoorwaarden van de Commandant Commando DienstenCentra en de Bestuursstaf;*
- j. *het mede begeleiden van relevant onderzoek in het kader van de Strategische kennis- en*
- k. *innovatieagenda (SKIA) en het mede waarborgen van de kwaliteit, tijdigheid, bruikbaarheid en defensiebrede beschikbaarheid van kennisproducten conform de eisen die zijn gesteld door en in afstemming met de desbetreffende beleidsverantwoordelijken;*
- l. *de informatievoorziening ten behoeve van de Commandant Commando DienstenCentra, gegeven het eigen terrein van verantwoordelijkheid;*
- m. *het leveren van: 1. medisch specialistische zorg, revalidatiezorg en geestelijke gezondheidszorg; 2. zorgcapaciteit (medisch specialistische en revalidatie) voor de opvang van (grotere aantallen) militaire en civiele slachtoffers; 3. militair geneeskundige opleidingen; 4. geneeskundige goederen, geneesmiddelen, geneeskundige uitrustingen, assemblage en diensten; 5. bloed en bloedproducten; 6. uitzendbaar medisch specialistisch personeel; 7. preventie en/of tijdige interventie op arbeidsrisico's, verzuimbegeleiding en (vroeg) reïntegratieactiviteiten om de inzetbaarheid van personeel te bevorderen en te behouden; 8. geneeskundige adviezen inzake de functie- c.q. dienstgeschiktheid van burgerambtenaren en militairen."*

Op grond van het subtaakbesluit (in het bijzonder artikel 4 sub b en c) is het verrichten van arbeidsmarktanalyses te kwalificeren als taak van DCPL.

Toepassingsbereik AVG

Materieel toepassingsbereik

Volgens de respondenten verwerkt de arbeidsmarktanalist geen persoonsgegevens bij het uitvoeren van een analyse. Dit komt omdat de aangeleverde en verzamelde data aan de voorkant geanonimiseerd is.

Wij merken hierbij het volgende op. De datasets die de analist gebruikt bij het uitvoeren van de analyses bevatten wél persoonsgegevens. Het is namelijk mogelijk om op basis van de aangeleverde datasets personen te identificeren. Een voorbeeld hiervan is een overzicht van DUO over het aantal afgestudeerde personen per studie. Daarin staat bijvoorbeeld dat één vrouw bij studie X aan universiteit Y is afgestudeerd in 2020. Een combinatie van deze gegevens zorgt ervoor dat dit indirect herleidbaar is tot een natuurlijk persoon. De Algemene verordening gegevensbescherming (hierna: AVG) bepaalt dat dit ook onder het materieel toepassingsbereik van de AVG valt. Naast de indirect herleidbare

persoonsgegevens verwerkt de arbeidsmarktanalist geen persoonsgegevens bij het uitvoeren van arbeidsmarktanalyses.

Aangezien er persoonsgegevens worden verwerkt valt het op grond van artikel 2 AVG binnen het materieel toepassingsbereik van de AVG.

Territoriale toepassingsbereik

Aangezien de verwerkingsverantwoordelijke – de Minister van Defensie – is gevestigd in Nederland, valt de verwerking van persoonsgegevens op grond van artikel 3 AVG ook binnen het territoriale toepassingsgebied van de AVG. De AVG is dus van toepassing op deze activiteit.

Beoordeling activiteit

DCPL houdt bij deze activiteit momenteel geen rekening met de beginselen van artikel 5 AVG. Dit komt omdat de medewerkers (waaronder de arbeidsmarktanalist) niet bewust zijn dat er persoonsgegevens worden verwerkt via de aangeleverde datasets. Er is geen invulling gegeven aan de volgende beginselen: rechtmatigheid, behoorlijkheid en transparantie, doelbinding, minimale gegevensverwerking, juistheid, opslagbeperking, integriteit en vertrouwelijkheid en de daaruit voortvloeiende verantwoordingsplicht. Voor de beoordeling bij deze activiteit beperken wij ons daarom tot een uitwerking van het beginsel van rechtmatigheid om te beoordelen of de activiteit überhaupt doorgang mag vinden. Aan de overige beginselen moet DCPL zelf nog invulling geven.

286

Rechtmatigheid

Iedere verwerking van persoonsgegevens moet op grond van artikel 5 lid 1 sub a AVG rechtmatig zijn. De rechtmatigheid is verder uitgewerkt in artikel 6 AVG. In dit artikel staan zes grondslagen op basis waarvan een verwerking rechtmatig is. We beperken ons in dit advies tot de meest voor de hand liggende grondslagen.

Algemeen belang

Artikel 6 lid 1 sub e AVG bepaalt dat persoonsgegevens mogen verwerkt als dat noodzakelijk is voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen. Deze taak moet wettelijk zijn vastgelegd. De taak moet daarnaast duidelijk en specifiek genoeg zijn omschreven dat het voor de betrokkene helder is dat er persoonsgegevens worden verwerkt en voor welk doel. Het is bovendien enkel toegestaan om de persoonsgegevens te verwerken die noodzakelijk zijn om die taak te vervullen. Deze activiteit kan op basis van de uit het subtaakbesluit voortvloeiende taken niet worden aangemerkt als een publieke taak voor het openbaar belang. De

taken zijn daarvoor niet specifiek genoeg omschreven. Het is voor de betrokkene namelijk niet te voorzien dat er persoonsgegevens worden verwerkt voor taken welke voortvloeien uit het subtaakbesluit. Met betrekking tot de rechtmatigheid kan DCPL daarom geen aansluiting vinden bij de grondslag algemeen belang. Een subtaakbesluit is namelijk niet als publieke taak te kwalificeren en de taakomschrijving is op zichzelf onvoldoende specifiek omschreven, waardoor niet voorzienbaar is dat het noodzakelijk en evenredig is om persoonsgegevens te verwerken om de taak uit te voeren. Bovendien is het subtaakbesluit een ministeriële regeling, waardoor het – zelfs als op basis van de taakomschrijving voldoende voorzienbaar is dat er persoonsgegevens worden verwerkt – geen bevoegdheid kan scheppen in de zin van artikel 6 lid 1 sub e AVG. Om een dusdanige taak en bevoegdheid te creëren is namelijk een wet in de formele zin vereist en een AOD, en in het verlengde daarvan een subtaakbesluit, missen deze rechtskracht.

Gerechtvaardigd belang

Op grond van artikel 6 lid 1 sub f AVG is een beroep op een gerechtvaardigd belang niet toegestaan bij de uitvoering van een publieke taak.¹²¹ In het geval dat het om een typisch bedrijfsmatige handeling voor een overheidsinstantie gaat is dit onder niet duidelijk gedefinieerde kaders wellicht een mogelijkheid. Daarnaast moet het verwerken van persoonsgegevens noodzakelijk en evenredig zijn, moet het een gerechtvaardigd belang van de verwerkingsverantwoordelijke zijn en moet dat belang prevaleren boven dat van de betrokkene. Een voorbeeld van een typisch bedrijfsmatige handeling van overheidsinstanties is het beveiligen van overheidsgebouwen. Een dergelijke bedrijfsmatige handeling wijkt namelijk niet af van private instanties die het gerechtvaardigd belang hebben hun eigendommen (waaronder panden) te beveiligen. Het is lastig om te beoordelen wat een typisch bedrijfsmatige handeling van een overheidsinstantie precies inhoudt. In de wet- en regelgeving, de literatuur en de rechtspraak is namelijk geen duidelijke definitie gegeven van een typisch bedrijfsmatige handeling van een overheidsinstantie.

Het uitvoeren van een arbeidsmarktanalyse met indirect herleidbare persoonsgegevens is volgens ons waarschijnlijk te kwalificeren als een taak ondersteunend aan de bedrijfsvoering van Defensie. Het uitvoeren van een arbeidsmarktanalyse met indirect herleidbare persoonsgegevens is volgens ons aan te merken als een typische bedrijfsmatige handeling, omdat Defensie zich hierin als overheidsinstantie niet wezenlijk van een private instantie onderscheidt. Het uitvoeren van een arbeidsmarktanalyse is daarnaast niet aan te merken als een publieke taak. Om die reden kan Defensie (als

¹²¹ Kamerstukken II 2017/18, 2034 851, nr.3, p. 37.

overheidsinstantie) mogelijk een beroep doen op de verwerkingsgrondslag gerechtvaardigd belang. Hiervoor is het wel noodzakelijk om het belang van Defensie af te wegen tegen het belang van de betrokkene. Defensie moet de gerechtvaardigd belang toets uitvoeren voor deze activiteit en deze ook vastleggen. Bovendien moet DCPL over het verwerken van persoonsgegevens helder informeren, bijvoorbeeld in de privacyverklaring van Defensie. Ook moet de verwerking noodzakelijk en evenredig zijn.

Mogelijk knelpunt	Aanbeveling
<i>Juridisch (beginselen artikel 5 AVG)</i>	
<p>1. Bij deze activiteit wordt momenteel geen rekening gehouden met de beginselen van artikel 5 AVG. Medewerkers zijn zich niet bewust dat er indirect herleidbare persoonsgegevens worden verwerkt en dat de AVG dus wel van toepassing is op deze activiteit.</p>	<p>Geef invulling aan de beginselen van artikel 5 AVG, aangezien er indirect herleidbare persoonsgegevens worden verwerkt.</p> <p>Bij de invulling van de rechtmatigheid kan daarbij mogelijk aansluiting worden gezocht bij de grondslag gerechtvaardigd belang. Het gaat namelijk om een zeer minimale inbreuk op de persoonlijke levenssfeer van de betrokkene. Het advies aan DCPL is om hiervoor de vereiste belangenafweging uit te voeren.</p> <p>Als DCPL invulling geeft aan de rechtmatigheid moet uiteraard ook rekening worden gehouden met de overige beginselen van artikel 5 AVG. De volgende acties vloeien daar onder andere uit voort:</p> <ol style="list-style-type: none"> 1. Neem de activiteit op in het verwerkingsregister; 2. Geef invulling aan de bewaartermijnen; 3. Zorg dat er niet meer persoonsgegevens worden verwerkt dan strikt noodzakelijk; 4. Zorg dat de persoonsgegevens alleen worden verwerkt voor het welbepaalde en uitdrukkelijk omschreven doel.

Conclusie

Op dit moment voldoet DCPL bij deze activiteit niet aan de beginselen van artikel 5 AVG. Dit komt omdat de medewerkers van DCPL niet bewust zijn dat er persoonsgegevens worden verwerkt. Het gaat weliswaar om indirect herleidbare persoonsgegevens, maar ook hierop is de AVG van toepassing. Het advies is om deze beginselen alsnog tegen het licht te houden bij deze activiteit. In het kader van de rechtmatigheid kan daarbij mogelijk aansluiting worden gezocht bij de grondslag gerechtvaardigd belang conform artikel 6 lid 1 sub f AVG. Als daarbij invulling wordt gegeven aan de rechtmatigheid en de overige beginselen van artikel 5 AVG kan deze activiteit mogelijk gewoon doorgang vinden. De activiteit kan waarschijnlijk op korte termijn doorgang vinden, mits wordt voldaan aan de beginselen van artikel 5 AVG. Daarom krijgt deze activiteit de kleur oranje.

Activiteiten 20 tot en met 22

Beschrijving activiteiten 20 tot en met 22

Geografische informatie (hierna: GI) is essentieel voor Defensie en voor het informatie gestuurd optreden (hierna: IGO). GI is doorgaans langzaam veranderende informatie die militairen kunnen gebruiken voor operaties. In alle domeinen en functies van militair optreden is geografische informatie noodzakelijk om te analyseren, te plannen en om situational awareness te krijgen. Defensie heeft drie GI-eenheden verantwoordelijke gemaakt:

De Dienst Geografie - activiteit 20

De Dienst Geografie (hierna: DGeo) heeft namens Defensie een convenant gesloten met het Kadaster waarmee de nationale geo-data voor Defensie beschikbaar is. Ook maakt het Kadaster specifieke militaire geografische producten voor Defensie. DGeo valt onder de landmacht en voert verschillende andere taken uit om te zorgen dat er voldoende wereldwijde data is:

a. Foundation Imagery

Dit zijn de lucht- en satellietfoto's die als basislaag dienen. Hierdoor beschikt Defensie als het ware over een eigen Google Maps. De resolutie is 60 centimeter voor stedelijke gebieden en 120 centimeter voor de buitengebieden. Dit betekent dat het niet mogelijk is om personen te identificeren. Ook zijn details, zoals kentekens, niet zichtbaar, omdat de foto's van bovenaf worden gemaakt.

Defensie heeft met verschillende commerciële partijen contracten gesloten, zodat zij deze informatie aangeleverd krijgen. Voorbeelden hiervan zijn Airbus en Maxar. Deze informatie is betrouwbaarder en veiliger dan bijvoorbeeld Google Maps. Dit komt omdat alles controleerbaar (datum opname, maker enzovoort) is. De kaarten zijn binnen MULAN voor iedereen beschikbaar.

b. Elevation & Relief

Er wordt hoogtedata verzameld. Deze informatie wordt steeds belangrijker in een militaire operatie. Voor de juiste situational awareness, line of sight berekeningen, simulatiesystemen, analyses en gedetailleerde hoogtecontouren en hoogtelijnen op een kaart, is deze data zeer belangrijk.

c. Topographic Information

Dit heeft betrekking op het beschikbaar stellen van topografische informatie, bijvoorbeeld kaarten, bij voorkeur op een schaal 1:50.000.

d. Aeronautical Information

De civiele luchtvaart heeft kaarten nodig met luchtvaartgegevens zoals vliegvelden, luchtruimen, luchtruimbeperingen, radio navigatie hulpmiddelen en obstakelinformatie. De militaire luchtvaart heeft in vredestrijd dezelfde verplichtingen als de civiele luchtvaart. Uit veiligheidsoogpunt moet ieder vliegtuig deze informatie zowel analoog als digitaal aanwezig hebben. Hier is DGeo voor verantwoordelijk.

Met betrekking tot deze gebieden verzamelt, beheert, produceert, publiceert en verspreidt DGeo GI en brengt zij advies uit over de verzamelde data. DGeo maakt GI toegankelijk voor de gehele Nederlandse Defensieorganisatie. Dit leidt tot situational awareness en uiteindelijk de voor besluitvorming benodigde situational understanding.

e. Human Geography Information

In 2018 heeft DGeo een studie uitgevoerd om de behoefte aan human geography data in kaart te brengen. Human geography gaat over relevante informatie voor militaire operaties zoals data over etniciteit, religie, groepen en organisaties, economie, talen enzovoort. Voor militairen is het van belang om deze informatie over een bepaald gebied op voorhand te hebben voordat ze daar bijvoorbeeld op missie gaan. Er is natuurlijk wel al over bepaalde gebieden geschreven, maar deze informatie is vaak verouderd. Defensie heeft behoefte aan actuele datalagen die gevisualiseerd worden op een kaart. Daarom heeft DGeo zich aangesloten bij een multinationalaal Defensie samenwerkingsverband om dit gezamenlijk uit te voeren. Dit programma heet het International Program Human Geography (hierna: IPHG).

Door de sociale lagen in kaart te brengen begrijpen militairen in wat voor gebied ze zitten. Zo weten ze bijvoorbeeld waar wel/geen mensen wonen, waar gezondheidscentra zitten, welke taal de bevolking spreekt of met wat voor mensen ze te maken krijgen. Op basis daarvan wordt de militaire capaciteit bepaald en wordt bijvoorbeeld een tolk ingeschakeld.

Binnen het IPHG wordt deze informatie op een kaart gevisualiseerd. Deze informatie wordt internationaal uitgewisseld. DGeo brengt enkel de informatie in beeld en analyseert dit niet. De inlichtingendienst voert wel analyses uit. Het gaat hierbij niet om verwerking van persoonsgegevens, omdat de groepen die in beeld worden gebracht daarvoor te groot zijn. Hierdoor is het niet mogelijk om natuurlijke personen te identificeren.

f. Soil – underground information

Momenteel loopt er een studie naar 'Underground information en soil'. Mocht uit deze studie naar voren komen dat er behoefte is aan underground information en soil dan zal DGeo zich hier in de toekomst ook mee bezighouden.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DGeo, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub I van het AOD bepaalt dat het Ministerie van Defensie de Commandant Landstrijdkrachten als verantwoordelijke kent.

292

Artikel 13 AOD bepaalt over de Commandant Landstrijdkrachten het volgende:

“De Commandant Landstrijdkrachten is belast met:

- a. Het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Landstrijdkrachten;*
- b. De gereedstelling en instandhouding van de landstrijdkrachten;*
- c. Het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. Het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstcentra op te leveren producten en diensten ter ondersteuning van het Commando Landstrijdkrachten;*
- e. De advisering op het gebied van militair landoptreden.”*

Artikel 26 AOD bepaalt dat de Commandant Landstrijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Landstrijdkrachten 2015

Artikel 2 lid 4 sub e subtaakbesluit bepaalt dat de Commando Landstrijdkrachten bestaat uit het Operationeel Ondersteuningscommando Land (hierna: OOL). Artikel 12 van het subtaakbesluit kent de volgende taken toe aan OOL:

“Het Operationeel Ondersteuningscommando Land staat onder leiding van de Commandant Operationeel Ondersteuningscommando Land die is belast met:

- a. het, met inachtneming van de aanwijzingen en de richtlijnen van de Commandant Landstrijdkrachten, geven van de ambtelijke leiding aan het Ondersteuningscommando Land;*
- b. het operationeel gereed stellen van eenheden en het in stand houden van de gereedheidstatus;*
- c. het formeren, inzet gereed stellen en bijdragen aan de instandhouding van operationeel gereede respectievelijk ingezette eenheden;*
- d. het uitvoeren van nazorg en recuperatie van operationeel ingezette eenheden;*
- e. het operationeel ondersteunen op het gebied van gevechtssteun, operationele logistieke ondersteuning en constructie, bij het gereed stellen van de eenheden van het CLAS;*
- f. het leveren van operationele ondersteuning aan alle grondtroepen van de krijgsmacht, waar ook ter wereld en bij nationale operaties;*
- g. het in voorkomend geval invulling geven aan de rol van Staf Detachement Nationale Operaties (SDNO);*
- h. het uitvoeren van regionale en/of lokale eerstelijns geneeskundige en tandheelkundige verzorging voor militair personeel;*
- i. het waarborgen van het veilig kunnen opereren van de onbemande vliegtuigsystemen;*
- j. het opsporen en opruimen van explosieven voor zowel Nationale Operaties als voor het expeditionair optreden van de krijgsmacht;*
- k. het ontwikkelen en onderhouden van kennisproducten/doctrines op het gebied van inlichtingen, vuursteun, explosievenopruiming en Civiel Militaire Interactie;*
- l. het ontwikkelen en verzorgen van opleidingen op het gebied van inlichtingen, vuursteun, explosievenopruiming en Civiel Militaire Interactie;*
- m. het uitvoeren van militaire bijstand en militaire steunverlening;*
- n. het leveren van een bijdrage aan de informatiebehoefte van de Commandant Landstrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid.”*

DGeo ontleent haar taken uit artikel 12 sub f, k en n van het subtaakbesluit.

Toepassingsbereik AVG

Materieel toepassingsbereik

DGeo verwerkt geen persoonsgegevens bij haar activiteiten. Om die reden valt de activiteit niet binnen het materieel toepassingsbereik van de Algemene verordening gegevensbescherming (hierna: AVG). De AVG is dus niet van toepassing. Om die reden komen we ook niet toe aan de toetsing van het territoriale toepassingsbereik van de AVG.

Wel is het volgende mogelijke knelpunt geconstateerd:

Mogelijk knelpunt		Aanbeveling
<i>Organisatorisch</i>		
1.	DGeo zit in vergelijking met andere NAVO lidstaten mogelijk op het verkeerde niveau in de organisatie 'weggestopt'. Bij bijna alle NAVO-landen zitten GI-diensten op het niveau van de inlichtingendienst. Het is van belang dat Defensieonderdelen tijdig informeren bij DGeo als zij bijvoorbeeld nieuw materiaal aankopen. Het moet namelijk wel mogelijk zijn om de GI (zoals kaarten) digitaal aanwezig te hebben in bijvoorbeeld vliegtuigen. Als het vliegtuig het systeem waarin Defensie werkt niet ondersteunt dan levert dit achteraf extra kosten op. Bij bijna ieder product is GI van belang, daarom moet er tijdig naar worden gekeken. Ook is er geen centrale leiding voor de drie GI-eenheden.	<p>Bepaal de positie van de GI-eenheden binnen de Defensieorganisatie. Ook kan het goed zijn om op centraal niveau deskundigen te positioneren. Vandaaruit kan een adviserende en sturende rol worden opgepakt.</p> <p>Ook is het belangrijk dat andere Defensieonderdelen bewust zijn van de noodzaak om de juiste geo data en standaarden te gebruiken. Vergroot de bewustwording op dit gebied onder Defensiepersoneel.</p>

De Dienst der Hydrografie - activiteit 21

De Dienst der Hydrografie (hierna: DHydro) is onderdeel van de marine en informeert zeevarenden over vaarwegen, de zeebodem en gevaren onder water, zoals scheepswrakken. DHydro heeft de wettelijke plicht om deze taak uit te voeren. DHydro maakt hiervoor zeekaarten, legt de zeegrenzen van Nederland daarin nauwkeurig vast, verricht dieptemetingen en maakt nautische producten. Hierdoor kunnen marineschepen en civiele schepen veilig

navigeren. Deze producten stelt DHydro ook beschikbaar op de commerciële markt.

DHydro beschikt over een aantal schepen. Daarvan vaart één schip permanent in de Noordzee en het Caribisch gebied om zeemetingen te verrichten. Ook gebruiken zij satellietfoto's van kustgebieden om de landsgrenzen te bepalen. De resolutie van deze foto's is 25 centimeter. De binnenwateren vallen niet onder de verantwoordelijkheid van DHydro. Daarvoor is Rijkswaterstaat verantwoordelijk.

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van DHydro, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

295

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub k AOD bepaalt dat het Ministerie van Defensie de Commandant Zeestrijdkrachten als verantwoordelijke kent.

Artikel 12 AOD bepaalt over de Commandant Zeestrijdkrachten het volgende:

“De Commandant Zeestrijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Zeestrijdkrachten;*
- b. de gereedstelling en instandhouding van de zeestrijdkrachten;*
- c. het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Zeestrijdkrachten;*
- e. het beheer van de Kustwacht Nederland en de Kustwacht Caribische Gebied;*
- f. de advisering op het gebied van militair maritiem optreden.”*

Artikel 26 AOD bepaalt dat de Commandant Landstrijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

Subtaakbesluit Commando Zeestrijdkrachten 2010

Artikel 2 lid 2 sub c subtaakbesluit bepaalt dat de Commando Zeestrijdkrachten bestaat uit de directie Operaties. Artikel 5 van het subtaakbesluit kent de volgende taken toe aan de directie Operaties:

“De directie Operaties staat onder leiding van de directeur Operaties die is belast met:

- a. het met inachtneming van de opdracht, planningskaders en (functionele) richtlijnen van de Commandant Zeestrijdkrachten geven van leiding aan de directie Operaties;*
- b. het ontwikkelen en onderhouden van maritiem-expeditionair vermogen in al zijn facetten;*
- c. het ontwikkelen en onderhouden van maritieme doctrines en tactieken;*
- d. het aanbrengen en behouden van de geoefendheid van enkelvoudige eenheden, samengestelde eenheden en een 'deployable' staf;*
- e. mede gelet op de taken van het Defensie Operatie Centrum, het, al dan niet als formerend Operationeel Commando, in opdracht en onder verantwoordelijkheid van de Commandant der Strijdkrachten uitvoeren van coördinerende activiteiten t.b.v. operaties;*
- f. het coördineren van de ondersteuning van eenheden die worden ingezet door de Commandant der Strijdkrachten, dan wel de Belgische Chief of Defense voor zover die inzet in binationaal verband en via de organisatie van de Admiraal Benelux wordt aangestuurd;*
- g. de operationele planning van operaties voorafgaande aan maar ook tijdens en na de operaties ten behoeve van het Defensie Operatie Centrum en het Belgische Center of Operations;*
- h. het geven van leiding aan de Dienst der Hydrografie en in dat kader uitvoeren van hydrografische, oceanografische en meteorologische ondersteuning bij militair optreden met daarnaast systematisch zeebodemonderzoek en nautische kartering overeenkomstig internationale verdragen;*
- i. het ontwikkelen en onderhouden van functionele richtlijnen - ten aanzien van het eigen terrein van verantwoordelijkheid - voor de gehele CZSK-organisatie;*
- j. het binnen het Commando Zeestrijdkrachten optreden als aanspreekpunt voor de directeur van de directie Operaties van de Defensiestaf;*

- k. *het leveren van een bijdrage aan de informatiebehoefte van de Commandant Zeestrijdkrachten, gegeven het eigen terrein van verantwoordelijkheid;*
- l. *de doelmatige inrichting, de bedrijfsvoering en het interne beheer van de directie Operaties."*

DHydro ontleent haar taken uit artikel 5 sub h van het subtaakbesluit Commando Zeestrijdkrachten 2010.

Toepassingsbereik AVG

Materieel toepassingsbereik

DHydro verwerkt geen persoonsgegevens bij haar activiteiten. Om die reden valt de activiteit niet binnen het materieel toepassingsbereik van de AVG. De AVG is dus niet van toepassing. Om die reden komen we ook niet toe aan de toetsing van het territoriale toepassingsbereik van de AVG.

Joint Meteo Groep - activiteit 22

De hoofdtak van Joint Meteo Group (hierna: JMG) is het maken van weersverwachtingen ten behoeve van de Nederlandse krijgsmacht. JMG valt onder de luchtmacht en richt zich op twee aspecten:

- a. Weersverwachtingen (Weather climate). Op dit gebied werkt JMG veel samen met het Koninklijk Nederlands Meteorologisch Instituut (hierna: KNMI);
- b. Ruimteweer (Space weather). Dit onderdeel is ook van belang om de troepen goed voor te bereiden. Een voorbeeld hiervan zijn de verstoringen van apparatuur door verschijnselen als het noorderlicht. Op het moment dat de krijgsmacht dit niet weet is het mogelijk dat ze denken dat de verstoringen door een vijand komen.

297

Taakomschrijving

Hieronder gaan wij in op de vraag in hoeverre deze activiteit valt onder de taken van JMG, zoals deze uit de verschillende wet- en regelgeving en interne inrichtingsbesluiten blijken. Met interne inrichtingsbesluiten worden het Algemeen organisatiebesluit Defensie (hierna: AOD) en subtaakbesluiten bedoeld.

Grondwet

Artikel 97 lid 1 Grondwet (hierna: Gw) bepaalt dat er een krijgsmacht is ten behoeve van de verdediging en ter bescherming van de belangen van het Koninkrijk, alsmede ten behoeve van de handhaving en de bevordering van de internationale rechtsorde. Artikel 97 lid 2 Gw voegt daaraan toe dat de regering het oppergezag heeft over de krijgsmacht.

Algemeen organisatiebesluit Defensie 2021

Artikel 1 sub m AOD bepaalt dat het Ministerie van Defensie de Commandant Luchtstrijdkrachten als verantwoordelijke kent.

Artikel 14 AOD bepaalt over de Commandant Luchtstrijdkrachten het volgende:

“De Commandant Luchtstrijdkrachten is belast met:

- a. het met inachtneming van de aanwijzingen van de Commandant der Strijdkrachten geven van leiding aan het Commando Luchtstrijdkrachten;*
- b. de gereedstelling en instandhouding van de luchtstrijdkrachten;*
- c. het binnen de gestelde normen en kaders leveren van – joint – producten en diensten ter ondersteuning van de overige Defensieonderdelen;*
- d. het binnen de gestelde normen en kaders uitoefenen van zeggenschap over de door de dienstencentra op te leveren producten en diensten ter ondersteuning van het Commando Luchtstrijdkrachten;*
- e. de advisering op het gebied van militair luchtoptreden.”*

Artikel 26 AOD bepaalt dat de Commandant Luchtstrijdkrachten op basis van het AOD een subtaakbesluit kan vaststellen ten aanzien van de eenheid waaraan hij leidinggeeft.

298

Subtaakbesluit Commando Luchtstrijdkrachten 2018

Artikel 2 lid 5 sub f subtaakbesluit bepaalt dat de operationele eenheden van de luchtmacht onder andere bestaat uit Vliegbasis Woensdrecht. Op deze vliegbasis is JMG gestationeerd. Verder worden er geen taken uiteengezet die toezien op JMG. Dit komt waarschijnlijk door de samenwerking met het KNMI en de wettelijke plicht die op het KNMI rust.¹²² Aangezien JMG geen persoonsgegevens verwerkt gaan we hier niet verder in op exacte taakstelling van JMG.

Toepassingsbereik AVG

Materieel toepassingsbereik

JMG verwerkt geen persoonsgegevens bij haar activiteiten. Om die reden valt de activiteit niet binnen het materieel toepassingsbereik van de AVG. De AVG is dus niet van toepassing. Om die reden komen we ook niet toe aan de toetsing van het territoriale toepassingsbereik van de AVG.

¹²² Deze wettelijke taken zijn vastgesteld in Wet taken meteorologie en seismologie en Regeling taken meteorologie en seismologie.

Conclusie

Bij de GI-activiteiten worden geen persoonsgegevens verwerkt. Het gaat namelijk om GI. Deze informatie is niet direct of indirect herleidbaar tot natuurlijke personen. Om die reden zijn er geen knelpunten geconstateerd die betrekking hebben op de AVG.

Bijlage 2 Persoonsgegevens per activiteit

In deze tabel staat per activiteit welke persoonsgegevens van elke soort kunnen worden verwerkt. Dit betekent niet dat bij elke verwerking alle persoonsgegevens altijd worden verwerkt. Verder willen we opmerken dat bij sommige activiteiten helemaal geen persoonsgegevens worden verwerkt. In het toelichtingenveld (rechtse kolom in de tabel) wordt in dat geval toegelicht om welke andere informatie het gaat.

#	Type persoonsgegevens			Toelichting
	Gewoon	Gevoelig	Bijzonder	
1	Naam, functie, geslacht		Politieke opvattingen, ras of etnische afkomst, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakbond, gezondheidsgegevens	
2	(gebruikers)-naam, profielfoto		Eventuele bijzondere persoonsgegevens die de betrokkene vrijwillig deelt	
3				Bij de ontwikkeling van de AI worden geen persoonsgegevens verwerkt.
4				Er worden geen persoonsgegevens verwerkt. Activiteit vindt altijd plaats in het kader van militaire bijstand,

				civiele autoriteit verwerkingsverantwoordelijke.
5A				Er worden geen persoonsgegevens verwerkt. Activiteit vindt altijd plaats in het kader van militaire bijstand, civiele autoriteit verwerkingsverantwoordelijke.
5B	Foto, functie, kenteken voertuig, naam	Video- en/of spraakopnamen	Biometrische gegevens	
6	Adres, e-mailadres, feiten/waarden over gedragingen, opmerkingen en/of eigenschappen, functie, geboortedatum, geslacht, IP-adres/MAC-adres, kenteken (voertuig)	Financiële gegevens	Gezondheidsgegevens, gegevens van strafrechtelijke aard, geloof, lidmaatschap vakbond, politieke opvattingen, seksuele gerichtheid.	
7	Adres, foto, e-mailadres, feiten/waarden over gedragingen, opmerkingen en/of eigenschappen, functie, geboortedatum, kenteken	Video- en/of spraakopnamen, financiële gegevens	Geloof, gezondheidsgegevens, lidmaatschap vakbond, politieke opvattingen, ras/ethniciteit, biometrische gegevens,	

	voertuig, IP-adres/MAC-adres, geslacht, naam		seksuele gerichtheid	
8	Adres, foto, e-mailadres, feiten/waarden over gedragingen, opmerkingen en/of eigenschappen, functie, geboortedatum, kenteken voertuig, IP-adres/MAC-adres, geslacht, naam	Video- en/of spraakopname, financiële gegevens	Geloof, gezondheidsgegevens, lidmaatschap vakbond, politieke opvattingen, ras/ethniciteit, seksuele gerichtheid	
9A	Locatiegegevens, IP-/MAC-adres, naam		Nationaliteit, religieuze of levensbeschouwelijke overtuigingen, politieke overtuigingen	Er worden geen persoonsgegevens verwerkt. De activiteit vindt (nog) niet plaats
9B	Naam, locatiegegevens, IP-/MAC-adres		Etnische afkomst, nationaliteit, religieuze of levensbeschouwelijke overtuigingen, politieke overtuigingen	Er worden geen persoonsgegevens verwerkt. De activiteit vindt (nog) niet plaats
10A	Naam, e-mailadres, foto, feiten/waarden over gedragingen,	Video- en/of spraakopname	Politieke opvattingen, ras of etnische afkomst, religieuze of levensbeschou	

	functie, geslacht		welike overtuigingen, lidmaatschap van een vakbond, gezondheidsge gevens, gegevens van strafrechtelijke aard, biometrische gegevens.	
10B	Naam, e- mailadres, foto, feiten/waarde ringen over gedragingen, functie, geslacht	Financiële gegevens, video- en/of spraakopnam e	Politieke opvattingen, ras of etnische afkomst, religieuze of levensbeschou welike overtuigingen, lidmaatschap van een vakbond, gegevens van strafrechtelijke aard, gezondheidsge gevens, biometrische gegevens.	
11	Naam			
12	e-mailadres, functie, geboortedatu m, geslacht, naam			
13				JIVC is zelf niet verantwoordelijk voor de persoonsgegevens die zij verwerken in de systemen die ze bouwen. Die

				hangt af van de opdrachtgever en het systeem dat ze moeten bouwen. Aangezien de categorieën persoonsgegevens dus afhankelijk zijn van de opdracht worden de persoonsgegevens hier niet verder uitgewerkt.
14A	Adres, e-mailadres, feiten/waarden over gedragingen, functie, geboortedatum, geslacht, IP-adres/MAC-adres, kenteken, naam, inloggegevens, foto	Financiële gegevens,	Foto, video-en/of spraakopname, geloof, gezondheidsgegevens, lidmaatschap vakbond, politieke opvattingen, seksuele gerichtheid	
14B	<zie vertrouwelijke bijlage>			
15	<zie vertrouwelijke bijlage>			
16	<zie vertrouwelijke bijlage>			
17	<zie vertrouwelijke bijlage>			
18	Adres, e-mailadres, feiten/waarden over gedragingen, functie, geboortedatum, geslacht, IP-adres/MAC-adres,	Financiële gegevens, Burgerservicenummer	Gezondheidsgegevens, gegevens van strafrechtelijke aard, geloof, politieke opvattingen, seksuele gerichtheid, (pas)foto	

19	Geslacht		Geloof, ras/ethniciteit	
20				Geografische informatie (hierna: GI) is essentieel voor Defensie en het informatie gestuurd optreden (hierna: IGO). In alle domeinen en functies van militair optreden is geografische informatie noodzakelijk om te analyseren, te plannen en om situational awareness te krijgen. De informatie is echter niet te herleiden tot een natuurlijk persoon. Er worden dus geen persoonsgegevens verwerkt.
21				Geografische informatie (hierna: GI) is essentieel voor Defensie en het informatie gestuurd optreden (hierna: IGO). In alle domeinen en functies van militair optreden is geografische informatie noodzakelijk om te analyseren, te plannen en om

				situational awareness te krijgen. De informatie is echter niet te herleiden tot een natuurlijk persoon. Er worden dus geen persoonsgegevens verwerkt.
22				Geografische informatie (hierna: GI) is essentieel voor Defensie en het informatie gestuurd optreden (hierna: IGO). In alle domeinen en functies van militair optreden is geografische informatie noodzakelijk om te analyseren, te plannen en om situational awareness te krijgen. De informatie is echter niet te herleiden tot een natuurlijk persoon. Er worden dus geen persoonsgegevens verwerkt.

Bijlage 3 Lijst van afkortingen en begrippen

In deze afkortingen- en begrippenlijst staan alle afkortingen en begrippen die in dit rapport en bijlagen zijn gebruikt. Dit zijn juridische afkortingen, Defensie specifieke afkortingen en gebruikte begrippen.

Lijst van afkortingen

Afkorting	Uitgeschreven
AED	Aanbieders van essentiële diensten
AGDEF	Aanwijzing Gereedstelling Defensie
AI	Artificial Intelligence
ANPR	Automatic Numberplate Recognition
AOD	Algemeen organisatiebesluit Defensie 2021
AOP	Centrum Arbeidsverhoudingen Overheidspersoneel
AST	Advanced Search teams
AVG	Algemene verordening gegevensbescherming
BS	Bestuursstaf
CBRN	Chemische, Biologisch, Radiologische en Nuclair
CBRN RE	Chemische, Biologisch, Radiologische en Nuclaire Respons Eenheid
NTC CBRN	Nationaal Trainingscentrum CBRN
CBS	Centraal Bureau voor de Statistiek
CD&E	Concept Development & Experimentation
CDC	Commandant DienstenCentra
CDS	Commandant der strijdkrachten
CDT'en	Commandanten (van de Operationele Commando's en overige Defensieonderdelen)
CEMA	Cyber and Electromagnetic Activities
CLAS	Commando Landstrijdkrachten
CLSK	Commandant Luchstrijdkrachten
COA	Centraal Orgaan opvang Asielzoekers
CPB	Centraal Plan Bureau
CSIRT	Computer security incident response team
CVE's	Common vulnerabilities and exposures
CZSK	Commando Zeestrijdkrachten
DAOG	Directie Aansturen Operationele Gereedstelling
DBB	Defensie Beveiligingsbeleid
DBBO	Defensie Bewaking- en Beveiligingsorganisatie
DCC	Defensie Cyber Commando
DCPL	Dienstcentrum Personeel & Logistiek
DCSC	Defensie Cyber Security Centrum
DGB	Directoraat Generaal Beleid
DGeo	Dienst Geografie

DHydro	Dienst der Hydrografie
DCo	Directie Communicatie
DMO	Defensie Materieel Organisatie
DO	Defensieonderdeel
DOPS	De Directeur Operaties
DOSCO	Defensie ondersteuning commando
DPIA	Data Protection Impact Assessment
DSP's	Digitale dienstverleners
DUO	Dienst Uitvoering Onderwijs
DV	Departementaal vertrouwelijk
EER	Europese Economische Ruimte
FFG	Follow-on Forces group
GI	Geografische Informatie
GMI	Geïntegreerd mobiel interceptieplatform
Gw	Grondwet
HDFC	Hoofddirectie Finance & Control
IED	Improvised explosive device
IFFG	Initial Follow-on Forces Group
IGO	Informatie gestuurd optreden
IM	Information Manoeuvre
IPHG	International Program Human Geography
JAT	Joint Arctic Training
JIVC	Joint InformatieVoorziening Commando
JMG	Joint Meteo Groep
JSC	Joint Support Cell
KD	Kerndepartement
KIXS	Kennis, Innovatie, eXperimenten en Simulatie
KMA	Koninklijke Militaire Academie
KMAR	Koninklijke Marechaussee
KNMI	Koninklijke Nederlands Meteorologisch Instituut
LIMC	Land Information Manoeuvre Centre
MIK	Maritiem Informatie Knooppunt
MinJ&V	Minister van Justitie en Veiligheid
MIVD	Militaire Inlichtingen & Veiligheidsdienst
MSOB	Militaire steunverlening in het openbaar belang
NCSC	Nationaal Cyber Security Centrum
NIS 2.0	Herziene richtlijn inzake de beveiliging van netwerk- en informatiesystemen
NLD SOCOM	Special Operations Command
NLDA	Nederlandse Defensie Academie
NRF	NATO Response Force
NTC CBRN	National trainingscentrum CBRN
OPSCEN	Operatie Centrum
OPSEC	Operational Security
OvJ	Officier van Justitie
Pw	Politiewet

RE	Respons Eenheid
SATG	Surface and Assault Training Group
SBB	Samenwerkingsverband Beroepsonderwijs
SG	Secretaris Generaal
SNA	Social Network Analysis
SNI	Social Network Influencing
TBB	Te Beschermen Belang
TESSOC	Terrorism Espionage Subversion Sabotage Organised Crime
TOS	Trends, Onderzoek en Statistiek
UAV	Unmanned aerial vehicle
UBR	Uitvoeringsorganisatie Bedrijfsvoering Rijk
VEVA	opleiding Veiligheids- en Vakmanschap
VJTF	Very High Readiness Joint Task Force
WBNI	Wet Beveiliging Netwerk- en Informatiesystemen
WenS	Werven en Selecteren
Wiv2017	Wet op de inlichtingen- en veiligheidsdiensten 2017

Definities

Begrip	Beschrijving
Pseudonimiseren	Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld. (Afkomstig uit artikel 4 lid 5 AVG).
Anonimiseren	Verwisseling van persoonsgegevens in gegevens die niet langer gebruikt kunnen worden om een natuurlijk persoon te identificeren, daarbij in ogenschouw nemende 'alle middelen die hiervoor redelijkerwijs gebruikt kunnen worden' door zowel een verantwoordelijke als een derde. De verwerking moet bovendien onomkeerbaar zijn. (Afkomstig van Werkroep 29).

Bijlage 4 Opzet onderzoek

Vorbereiding

Ter voorbereiding op het onderzoek is gestart met analyseren van specifieke privacywetgeving die van toepassing is op Defensie, zoals de Regeling Gegevensbescherming Militaire Operaties en andere relevante (militaire) wetgeving. Hierbij is gebruik gemaakt van materiedeskundigen van Defensie. Naar aanleiding van de input is de wetgeving verder geanalyseerd en zijn de kaders¹²³ bepaald die relevant zijn voor het vervolg van de opdracht.

Scope bepaling

In de tweede nota van inlichtingen heeft Defensie aangegeven dat het gaat om een inventarisatie, de QuickScan, van veertig activiteiten (40) verspreid over twintig organisatiedelen. Bij start van het project en gedurende het project is door Defensie de QuickScan nogmaals beoordeeld en bleek dat het aantal activiteiten uiteindelijk kon worden vastgesteld op tweeëntwintig (22) activiteiten verspreid over acht OPCO's. Deze wijziging kwam onder meer doordat sommige activiteiten buiten de scope¹²⁴ van de opdracht vallen en een onjuiste vernummering van de activiteiten in de QuickScan. Van deze activiteiten zijn er 10 activiteiten gerubriceerd als Departementaal Vertrouwelijk (hierna: DV). Defensie heeft de QuickScan geprioriteerd en nader toegelicht aan EIFFEL, alvorens EIFFEL gestart is met de beoordeling van de activiteiten.

310

Interviews afnemen

Na de voorbereiding zijn interviews gepland met de respondenten. Hierbij legde Defensie het eerste contact met de Point of Contact (hierna: POC) van het betreffende onderdeel en bracht deze in contact met de POC van EIFFEL. Vervolgens kon vaak op korte termijn een interview worden gepland tussen de kennishouders en de onderzoekers van EIFFEL. De interviews met de respondenten hebben voornamelijk fysiek op locatie plaatsgevonden, enkele interviews hebben telefonisch of via MTeams plaatsgevonden (alleen indien er geen sprake was van DV- activiteiten). Per activiteit zijn één of meerdere gesprekken gevoerd. Tijdens deze interviews stond de betreffende activiteit centraal: wat houdt de activiteit exact in, hoe ziet het proces eruit en welke mogelijke knelpunten worden ervaren door de respondent. De interviews gaven

¹²³ Artikel 5 AVG

¹²⁴ Programma van Eisen onderdeel 4: 1) De scope van dit onderzoek is beperkt tot het verwerken van gegevens ten behoeve van de eigen taken van Defensie en/of de krijgsmacht. Het verspreiden van informatie naar en beïnvloeden van actoren buiten defensie in een informatieomgeving zijn buiten scope. 2) De reikwijdte is beperkt tot het verwerken van gegevens op Nederlands nationaal grondgebied (inbegrepen marineschepen).

daarmee inzicht in mogelijke knelpunten vanuit juridisch, maar ook organisatorisch en ethisch perspectief.

Analyse mogelijke knelpunten

Op basis van de mogelijke knelpunten die naar voren kwamen tijdens de interviews, is nader onderzoek verricht door de specialisten van EIFFEL. Ook zijn de activiteiten getoetst aan de beginselen van de AVG.¹²⁵

Hierbij is integraal gewerkt. Dit houdt in dat alle specialisten op de hoogte zijn van elkaars juridische dilemma's bij de verschillende activiteiten, inzichtelijk is welke dilemma's eventueel OPCO of eenheid overstijgend zijn of wanneer wet- en regelgeving tegenstrijdig is aan elkaar. In deze fase schakelden de experts van EIFFEL met de materiedeskundigen van Defensie, om te toetsen of onze analyse aansluit bij de militaire context. Vervolgens zijn alle activiteiten, mogelijke knelpunten en aanbevelingen uitgewerkt in dit rapport.

¹²⁵ Artikel 5 AVG

Bijlage 5 Programma van Eisen

behorende bij referentienummer 19436041

1. Inleiding

De Functionaris Gegevensbescherming AVG Defensie heeft recent een onderzoek uitgevoerd bij het experimentele Land Information Manoeuvre Centre (LIMC) van de Koninklijke Landmacht naar de naleving van de Algemene Verordening Gegevensbescherming (AVG) bij het verwerken van persoonsgegevens (zie bijlage I). Bij Defensie bestaat behoefte aan externe capaciteit om bij nog een aantal andere onderdelen/eenheden te onderzoeken in hoeverre de AVG daar wordt nageleefd bij het verwerken van persoonsgegevens. Daarbij is het van belang om voor die activiteiten waarbij de gegevensverwerking niet in overeenstemming met de AVG zou zijn, maatregelen te treffen om de AVG alsnog na te leven, zodat de bedrijfsvoerings- en operationele processen binnen de kaders van de wet- en regelgeving doorgang kunnen vinden.

Daarnaast heeft de Krijgsmacht handelingsperspectief nodig om i.h.k.v. de operationele taken op te kunnen treden in de informatieomgeving. Dit is nodig om te kunnen oefenen en trainen, tijdig te kunnen anticiperen op (hybride) dreigingen en inzet en voor het beveiligen van defensieobjecten. Indien tijdens het onderzoek blijkt dat er in het kader van de bedrijfsvoering of in het kader van de personele, materiële en operationele gereedstelling (oefenen en trainen) activiteiten worden uitgevoerd die niet binnen de geldende juridische kaders mogelijk zijn, wordt gevraagd dit per geval aan de opdrachtgever voor te leggen en te adviseren over het oplossen van de knelpunten.

312

2. Probleemschets

Defensie heeft 3 hoofdtaken¹²⁶ die voortkomen uit de grondwet (art 97). Binnen deze hoofdtaken kan de krijgsmacht in (inter)nationaal verband worden ingezet met inachtneming van (inter)nationale wet- en regelgeving. Het moment waarop, de grondslag waarbinnen activiteiten worden uitgevoerd (oefenen en trainen of inzet), de plaats van de activiteiten (binnen- of buitenland) en de omstandigheden (vredestijd of oorlog) zijn medebepalend voor wat volgens de juridische kaders wel en niet mag.

¹²⁶ 1. bescherming (bondgenootschappelijk) grondgebied 2. beschermen en bevorderen van de internationale rechtsorde 3. ondersteunen civiele autoriteiten).

Informatiegestuurd optreden is nu en met het oog op de toekomst (zie bijgevoegde Defensievisie2035) een centraal thema. De technologische mogelijkheden en strategische noodzaak om behalve in de fysieke dimensie ook in de virtuele of cognitieve dimensie van de informatieomgeving te oefenen en opereren, nemen toe. Diverse actoren, waaronder landen en terroristische organisaties, die informatie nu al als wapen gebruiken treden echter vaak buiten de voor ons aanvaardbare kaders. Wanneer dit soort actoren ongehinderd en ongezien kunnen optreden in onze informatiesamenleving kan dat leiden tot ondermijnen van overheidsgezag, plegen van aanslagen, saboteren van vitale infrastructuur of andere vormen van ernstige maatschappelijke ontwrichting. Uiteraard moeten we, net als bij de toepassing van geweld, ons daarbij houden aan de bestaande juridische kaders, alwaar de AVG deel van uitmaakt. Het probleem is dat er bij uitvoerende eenheden onvoldoende inzicht is in de mogelijkheden en grenzen van juridische kaders op dit vlak en nog onvoldoende is geïdentificeerd wanneer en hoe de juridische kaders de taakuitvoering beperken.

In het kader van het gevraagde onderzoek gaat het om activiteiten in Nederland, in vreedstijd en het betreft zowel bedrijfsvoeringsactiviteiten als de gereedstelling en eventuele inzet in Nederland. Voor inzet van de krijgsmacht in Nederland geldt specifieke wet- en regelgeving (zie daartoe de in bijlage II gevoegde notitie van DJZ).

313

3. Doelstelling en onderzoeksvragen

De doelstelling van het onderzoek is tweeledig:

1. Inventariseer verwerkingen met persoonsgegevens bij eenheden/onderdelen van Defensie waarbij op basis van de eerder uitgevoerde quick-scan twijfel bestaat of de beginselen van de AVG in voldoende mate worden nageleefd.
2. Inventariseer, op basis van een selectie uit de eerder uitgevoerde quick-scan, de door de eenheden/onderdelen (gepercipieerde) juridische knelpunten voor de uitvoering van hun taken en doe aanbevelingen voor het oplossen van bestaande knelpunten.

Tenminste de volgende onderzoeksvragen moeten hiertoe worden beantwoord:
Voor subdoelstelling 1:

- In hoeverre is er bij de onderdelen/eenheden sprake van verwerking van persoonsgegevens waarbij twijfel bestaat of de beginselen inzake de verwerking van persoonsgegevens van de AVG worden nageleefd? Specificeer op basis van:

- o Rechtmatigheid.
 - o Behoorlijkheid en transparantie.
 - o Doelbindingsbeginsel.
 - o Beginsel van dataminimalisatie.
 - o Juistheidsbeginsel.
 - o Beginsel van opslagbeperking.
 - o Beginsel van integriteit en vertrouwelijkheid.
 - o Verantwoordingsplicht.
- Welke aanbevelingen kunnen, in voorkomend geval, worden gedaan voor het naleven van de AVG?

Voor subdoelstelling 2:

- In hoeverre is er bij de onderdelen/eenheden sprake van knelpunten in de taakuitvoering die voortvloeien uit naleven van overige vigerende juridische kaders voor optreden in de informatieomgeving? Specificeer de geconstateerde knelpunten.
- Welke aanbevelingen kunnen worden gedaan voor oplossen van de (gepercipieerde) knelpunten binnen de vigerende juridische kaders?

4. Scope/Reikwijdte

- De scope van dit onderzoek is beperkt tot het verwerken van gegevens ten behoeve van de eigen taken van Defensie en/of de krijgsmacht. Het verspreiden van informatie naar en beïnvloeden van actoren buiten defensie in een informatieomgeving zijn buiten scope.
- De reikwijdte is beperkt tot het verwerken van gegevens op Nederlands nationaal grondgebied (inbegrepen marineschepen).
- Van belang is dat bij de inventarisatie van informatie-activiteiten duidelijk onderscheid gemaakt wordt tussen verwerking in het kader van een van de (hoofd)taken van de krijgsmacht en verwerking in het kader van de bedrijfsvoering.