Functionaris voor Gegevensbescherming

Onderzoek naleving Algemene verordening gegevensbescherming

Experimenteeromgeving Land Information Manoeuvre Centre (LIMC)

Datum	31-3-2021
Status	Definitief
Nummer	BS2021004839

Colofon

Contactpersoon	mr. O.L. Stenhuis-Kok Functionaris voor Gegevensbescherming Avg Defensie
Opdrachtgever	Functionaris voor Gegevensbescherming Avg Defensie
Rubriceringstermijn	Gederubriceerd
Errata	Pagina 54 en 73: 80 in plaats van 89 rapporten zijn geanalyseerd. Pagina 48: aangetroffen in plaats van gesloten Avg verwerkersovereenkomst

Voorwoord

De Functionaris voor Gegevensbescherming (FG) fungeert als de wettelijke interne toezichthouder op de naleving van de geldende wet- en regelgeving ter bescherming van persoonsgegevens.

Naar aanleiding van mediaberichten over vermeende onregelmatigheden bij het verzamelen en analyseren van informatie rond de COVID-19 crisis door het *Land Information Manoeuvre Centre* (LIMC) van de Koninklijke Landmacht heb ik een onderzoek geïnitieerd naar de naleving van de Algemene verordening gegevensbescherming (Avg).

Voor de uitvoering van het onderzoek is een onderzoeksteam geformeerd met de volgende personen:

- mr. O.L. Stenhuis-Kok, Functionaris Gegevensbescherming Avg
- [redacted], Functionaris Gegevensbescherming Wpg
- [redacted], Avg coördinator defensiebrede verwerkingen
- [redacted], advies en ondersteuning
- functionaris Beveiligingsautoriteit

Ondanks de COVID-19 maatregelen waaronder dit onderzoek heeft plaatsgevonden vind ik het belangrijk te benadrukken, dat de gesprekken met de medewerkers en leidinggevenden werkzaam bij de Koninklijke Landmacht - en het LIMC in het bijzonder - in een open atmosfeer hebben plaatsgevonden. Ik dank hen voor de constructieve medewerking.

Tijdens het onderzoek heeft het onderzoeksteam advies en ondersteuning ontvangen van medewerkers van de Inspectie Veiligheid Defensie, de afdeling Trends Onderzoek en Statistiek en de Autoriteit Persoonsgegevens.

Tot slot een woord van dank aan de leden van het onderzoeksteam en de overige kritische meelezers van deze rapportage.

De Functionaris voor Gegevensbescherming Avg Defensie,

Olga Stenhuis-Kok

Inhoud

Samenvatting

Aanleiding

NRC Handelsblad bericht op 16 november 2020 over de activiteiten van het *Land Information Manoeuvre Centre* (LIMC). Defensie heeft hierop gereageerd. Uit de berichtgeving en de reacties daarop komt het beeld naar voren dat bij het LIMC mogelijk sprake is van incidenten bij het verwerken van persoonsgegevens. Als Functionaris voor Gegevensbescherming (FG) heb ik daarop als onafhankelijk intern toezichthouder binnen het ministerie van Defensie besloten een onderzoek in te stellen naar de naleving van de Algemene verordening gegevensbescherming (Avg) in het kader van door het LIMC uitgevoerde activiteiten. Dit rapport doet hiervan verslag.

Het LIMC is onder commando gesteld van het Operationeel Ondersteuningscommando Land (OOCL), een onderdeel van de Koninklijke Landmacht.

Onderzoeksvragen

Centrale onderzoeksvraag

Heeft het ministerie van Defensie in het kader van de door de experimenteeromgeving LIMC uitgevoerde activiteiten gehandeld in overeenstemming met de Avg, de Uitvoeringswet Avg (UAvg) en de Regeling Avg Defensie?

Deelvragen

Om antwoord te kunnen geven op de centrale onderzoeksvraag zijn zeven deelvragen opgesteld:

1. Zijn er binnen het ministerie van Defensie in het kader van de door de experimenteeromgeving LIMC uitgevoerde activiteiten persoonsgegevens verwerkt zoals bedoeld in de artikelen 2, 4 lid 1 en lid 2 Avg? Is het verwerken van informatie uit openbaar toegankelijk bronnen in overeenstemming met de Avg beoordeeld, gekwalificeerd en ingericht?

2. Zijn er binnen het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten bijzondere categorieën van persoonsgegevens verwerkt zoals bedoeld in artikel 9 Avg? Bijvoorbeeld gegevens betreffende de gezondheid en gegevens betreffende politieke, religieuze of levensbeschouwelijke overtuiging?

3. Indien er binnen het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten verwerkingen van persoonsgegevens hebben plaatsgevonden, met welk welbepaald en omschreven doel hebben de minister van Defensie en de Commandant Landstrijdkrachten deze persoonsgegevens verwerkt en konden de verwerkingen op een rechtmatige grondslag zoals omschreven in de artikelen 6 en 9 Avg worden gebaseerd?

4. Vast te stellen of en zo ja welke personen onder het gezag of in opdracht van het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten persoonsgegevens hebben verwerkt of waar persoonsgegevens aan zijn verstrekt en op welke wijze de logging, autorisatie en toegang tot geautomatiseerde systemen en gegevensbronnen was ingericht. En tevens vast te stellen of het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten aan personen of instanties buiten het ministerie van Defensie persoonsgegevens heeft verstrekt en zo ja, met welk doel dat is gebeurd.

5. Diende het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde verwerkingsactiviteiten een melding op te nemen in het Avg verwerkingenregister Defensie en zo ja, is deze melding gedaan?

6. Was vooraf voor het ministerie van Defensie met het oog op de door de experimenteeromgeving LIMC uit te voeren activiteiten het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) op het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens zoals bedoeld in artikel 35 Avg vereist en zo ja, is er een DPIA uitgevoerd?

7. Welke technische en organisatorische maatregelen zijn door het ministerie van Defensie getroffen ter beveiliging van de in het kader van de door de experimenteeromgeving LIMC uitgevoerde activiteiten verwerkte (persoons)gegevens, zoals bedoeld in artikel 32 Avg en zoals uitgewerkt in Defensie beveiligingsbeleid (DBB)?

Onderzoekaanpak

Op 18 november 2020 is aan de Commandant Landstrijdkrachten, in zijn rol als Avg Beheerder, meegedeeld dat er aan het LIMC in 't Harde toezichtbezoeken worden afgelegd. Hierbij zijn verkennende gesprekken gevoerd met diverse bij het LIMC betrokken medewerkers en leidinggevenden. Het beeld dat uit de eerste oriëntatiefase naar voren kwam toonde aan dat persoonsgegevens zijn verwerkt maar dat de activiteiten hier niet op waren gericht.

Na de toezichtbezoeken is een onderzoeksteam geformeerd en een plan van aanpak opgesteld. Naast de toezichtbezoeken op locatie is een documentenanalyse uitgevoerd, is een enquête onder (oud) medewerkers van het LIMC uitgevoerd en zijn interviews gehouden.

Afbakening

Het onderzoek richt zich op door het LIMC uitgevoerde activiteiten in de periode vanaf de oprichting op 23 maart 2020 tot en met 27 november 2020. Op 27 november heeft de minister van Defensie besloten de activiteiten van het LIMC voor wat het verzamelen en analyseren van informatie betreft stil te zetten.

Het onderzoek richt zich op de vraag of de activiteiten die door het LIMC in deze periode zijn uitgevoerd in overeenstemming waren met de (U)Avg en Regeling Avg Defensie. In het bijzonder gaat het om de vraag of in strijd hiermee persoonsgegevens zijn verwerkt. Een persoonsgegeven is elke informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De FG formuleert daarover conclusies en, indien de bevindingen daartoe aanleiding geven, aanbevelingen. Het

onderzoek richt zich niet op de bredere ontwikkelingen op het gebied van informatie gestuurd optreden binnen de krijgsmacht, bij andere defensieonderdelen of CD&E (*concept development & experimentation*) projecten buiten het LIMC.

Conclusies

Op basis van het toetsingskader zijn bevindingen beoordeeld. Dit heeft geleid tot onderstaande conclusies en aanbevelingen.

1. Vastgesteld is dat het LIMC persoonsgegevens heeft verwerkt. Dit gebeurde niet grootschalig en zonder de intentie om persoonsgegevens te verwerken. Het LIMC heeft COVID-19 gerelateerde maatschappelijke ontwikkelingen als "fenomeen" in kaart gebracht om militaire en civiele besluitvorming te voeden met inzicht en handelingsperspectief.

   Het LIMC heeft gegevens uit algemeen toegankelijke bronnen, waaronder nieuwswebsites en sociale mediaplatforms, verzameld, geanalyseerd en verwerkt in rapportages. Lang niet in alle gevallen ging het daarbij om persoonsgegevens, maar bijvoorbeeld om statistische gegevens van IC-opnames en besmettingsaantallen. Het uitvoeren van zoekopdrachten en het raadplegen van persoonsgegevens via het internet zijn wel verwerkingen en vallen dus onder het toepassingsbereik van de Avg.

   Het onderzoek heeft daarnaast aangetoond dat in de rapportages nog persoonsgegevens van (publieke) personen voorkomen. Ook het tijdens of voorafgaand aan het analyse- en productieproces verwijderen van persoonsgegevens uit de rapporten ('pseudonimiseren'), is een verwerking van persoonsgegevens en ook daarop is de Avg van toepassing. Sommige persoonsgegevens zoals die van publieke figuren en bronvermeldingen zijn in rapportages opgenomen omdat medewerkers van het LIMC na verkregen advies dachten dat dit volgens de Avg was toegestaan. Vastgesteld is dat hierover overleg heeft plaatsgevonden en dat het LIMC op dit punt onjuist advies heeft ontvangen.

2. Vastgesteld is dat het LIMC bijzondere persoonsgegevens heeft verwerkt, dit betreft persoonsgegevens over politieke opvattingen. Het gaat om namen en functies van bekende politici en bestuurders. In voorkomende gevallen zal het gaan om bijzondere persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. De doorbrekingsgrond: kennelijke openbaarheid door de betrokkene, zou mogelijk van toepassing zijn als de wettelijke grondslag voldeed. Andere bijzondere categorieën van persoonsgegevens zijn door het onderzoeksteam niet aangetroffen. De interviews en de enquête uitkomsten bevestigen dit.

3. Het doel van de verwerking is vooraf omschreven in de operatiebevelen van de Commandant Landstrijdkrachten en de Commandant Operationeel Ondersteuningscommando Land. In het kort: militaire en civiele besluitvorming voeden met inzicht en handelingsperspectief in relatie tot COVID-19. Dit doel is gezien de context voldoende welbepaald, maar niet gerechtvaardigd omdat de wettelijke grondslag ontbreekt zoals bedoeld in artikel 6, eerste lid, Avg. De verwerking voldoet daarmee ook niet aan het rechtmatigheidsbeginsel, als bedoeld in artikel 5 Avg. Het civiel gezag heeft geen verzoek gedaan om militaire bijstand of militaire steunverlening in het openbaar belang (MSOB) en de minister van Defensie heeft geen zelfstandige taak en/of bevoegdheid waarop de nationale inzet van het LIMC kan berusten.

4. Het LIMC was en is geen organieke eenheid binnen het CLAS. Medewerkers zijn dan ook niet geplaatst bij het LIMC maar voor korte of langere tijd vanuit bestaande eenheden of organisaties gevraagd of aangewezen om activiteiten te verrichten.

   De logging, autorisatie en toegang tot systemen en gegevensbronnen is bij het LIMC ingericht conform de stringente normen van het Defensiebeveiligingsbeleid (DBB).

   Informatieproducten van het LIMC zijn zowel binnen als buiten Defensie verspreid. De verzendlijst bevat maximaal 94 geadresseerden, waarvan ongeveer de ene helft e-mailadressen binnen het ministerie van Defensie en andere helft overheidsinstanties buiten Defensie. Er was geen grondslag of taak voor de nationale inzet van het LIMC ten behoeve van civiele autoriteiten. Er was geen grondslag om producten van het LIMC die persoonsgegevens bevatten te verstrekken aan personen of instanties binnen of buiten het ministerie van Defensie.

5. Omdat persoonsgegevens werden verwerkt was een melding van deze activiteiten in het Avg verwerkingenregister Defensie noodzakelijk. Deze melding is niet gedaan.

6. De Avg-regelgeving schrijft voor dat ook bij een beleidsinitiatief, zoals het concept *Information Manoeuvre*, voorafgaand aan de verwerking een DPIA vereist is. Dit is niet gebeurd.

7. De normen van het DBB zijn nageleefd voor wat betreft organisatorische maatregelen als geheimhoudingsverklaring, beveiligingsbriefing en screening. Op het gebied van technische maatregelen is vastgesteld dat bij *throughput* en *output* gebruik is gemaakt van geaccrediteerde informatiesystemen waarmee ruimschoots is voldaan aan de norm. Voor *input* is vastgesteld dat naast geaccrediteerde informatiesystemen gebruikgemaakt van een privé laptop met beveiligingsmaatregelen die niet aantoonbaar voldoen aan de norm.

Eindconclusie

Het LIMC heeft COVID-19 gerelateerde maatschappelijke ontwikkelingen als "fenomeen" in kaart gebracht om militaire en civiele besluitvorming te voeden met inzicht en handelingsperspectief. Het LIMC had niet de intentie om (grootschalig) persoonsgegevens te verwerken, maar is hierin niet volledig geslaagd. Persoonsgegevens kwamen mee als "bijvangst".

Voor deze verwerking bestond geen wettelijke grondslag en is niet voldaan aan de verantwoordingsplicht waardoor de Avg onvoldoende is nageleefd.

Aanbevelingen

De Functionaris Gegevensbescherming beveelt de minister van Defensie aan:

1. *Stel een (beleids-) DPIA op voor Informatiegestuurd optreden*
   In de Defensievisie 2035 is Informatiegestuurd optreden (IGO) de basis van de toekomstige defensieorganisatie. Het verwerken van persoonsgegevens is hierbij onvermijdelijk. Soms valt de verwerking van persoonsgegevens onder de Wet inlichtingen- en veiligheidsdiensten 2017, de Wet politiegegevens of is een uitzondering voor inzet van de krijgsmacht aan de orde waardoor de Avg materieel niet van toepassing is. Bij andere verwerkingen van persoonsgegevens is de Avg wel van toepassing. Gezien de soort van de verwerking is een hoog privacyrisico waarschijnlijk en is daarom een (beleids-)DPIA vereist.

2. *Actualiseer de Catalogus Nationale Operaties 2018*
   Wet- en regelgeving bepaalt de mogelijkheden voor de inzet van de krijgsmacht, ook bij nationale taken. Afspraken over de beschikbare capaciteit en aanvraagprocedures voor civiel-militaire samenwerking zijn onder meer vastgelegd in de Catalogus Nationale Operaties 2018. Die biedt een overzicht van de inzetmogelijkheden van de krijgsmacht op Nederlands grondgebied door middel van steunverlening en bijstand aan de overheid. Het verdient aanbeveling om bij de volgende actualisatie van de catalogus daarin een omschrijving van de taken, verantwoordelijkheden, bevoegdheden en mogelijkheden van de krijgsmacht op het gebied van *information manoeuvre* en andere militaire analysecapaciteit op te nemen.

3. *Hanteer willen, mogen en kunnen in de juiste volgorde*
   Ontwikkelingen bij de krijgsmacht moeten binnen de kaders van wet- en regelgeving de (technische) mogelijkheden en het beoogde doel worden beschouwd. Met andere woorden, vragen in verband met willen, mogen en kunnen moeten in de juiste volgorde worden gesteld én beantwoord. Indien behoefte bestaat aan wijziging van regelgeving, bijvoorbeeld door ontwikkelingen in het informatiedomein, is wetgeving vereist. Voordat deze behoefte wordt overwogen is het antwoord op de "willen" vraag noodzakelijk.

4. *Versterk de poortwachtersfunctie op het gebied van gegevensverwerking*
   Verhoog bij behoeftestellers en inkopers structureel het risicobewustzijn van het verwerken van persoonsgegevens bij de verwerving van *webbased* producten en diensten ten behoeve van het informatiedomein. Maak, zoals voorgeschreven, gebruik van de model Avg verwerkersovereenkomsten.

5. *Inventariseer risicovolle verwerkingen van persoonsgegevens*
   Inventariseer in 2021 verwerkingen met persoonsgegevens bij Defensie waarbij getwijfeld wordt of de principes van de Avg in voldoende mate worden nageleefd en prioriteer deze mede aan de hand van de DPIA criteria in de Avg.

6. *Versterk en professionaliseer de Avg organisatie*
   Versterk en professionaliseer de Avg organisatie en schenk daarbij in het bijzonder aandacht aan de Avg coördinatiefunctie en aan de samenwerking met de juridische en operationele lijn. Voorzie in een risicogerichte invulling van de Avg-organisatie door bij eenheden zoals OOCL/JISTARC fysiek een Avg-coördinator onder te brengen. Geef in samenspraak met de FG invulling aan de functie van een *Chief Privacy Officer (CPO)*[1] en positioneer deze binnen de BS/DBE.

[1] Naar analogie van de motie van het lid Verhoeven c.s. over een chief privacy officer bij uitvoeringsorganisaties. Kamerstukken II 2020/21, 27529 nr. 239

1 Inleiding

1.1 Aanleiding

NRC Handelsblad bericht op 16 november 2020 over de activiteiten van het *Land Information Manoeuvre Centre* (LIMC). Defensie heeft hierop gereageerd.[2] Uit de berichtgeving en de reacties daarop komt het beeld naar voren dat bij het LIMC mogelijk sprake is van incidenten bij het verwerken van persoonsgegevens. Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[3] De Functionaris voor Gegevensbescherming (FG) heeft daarop als onafhankelijk intern toezichthouder binnen het ministerie van Defensie besloten een onderzoek in te stellen naar de naleving van de Algemene verordening gegevensbescherming (Avg) door LIMC. Dit rapport doet hiervan verslag.

1.2 Algemene onderzoeksgegevens

Op 18 november 2020 heeft de FG schriftelijk bij de Commandant Landstrijdkrachten (C-LAS) aangekondigd op zo kort mogelijke termijn een toezichtbezoek uit te voeren bij het LIMC (bijlage I). Het LIMC is onder commando gesteld van het Operationeel Ondersteuningscommando Land (OOCL) een onderdeel van het Commando Landstrijdkrachten (CLAS).

Het onderzoeksteam heeft op 19 november, 24 november en 1 december 2020 toezichtbezoeken afgelegd bij het LIMC om een eerste beeld te krijgen van de verwerkingsactiviteiten. Hierbij zijn verkennende gesprekken gevoerd met diverse bij het LIMC betrokken medewerkers en leidinggevenden. Het LIMC en OOCL hebben hieraan volledige medewerking en ondersteuning verleend. Het onderzoeksteam is rondgeleid in de werkruimtes en is nader geïnformeerd over diverse aspecten zoals de organisatiestructuur en bedrijfsvoering, de uitgevoerde werkzaamheden, de geautomatiseerde werkomgeving en de gebruikte gegevensbronnen. Het onderzoeksteam heeft inzage gekregen in processen en systemen. Het LIMC heeft een aantal processen van de gehanteerde werkwijze uitgelegd, getoond en gedemonstreerd. Het beeld dat uit de eerste oriëntatiefase naar voren kwam toonde aan dat persoonsgegevens zijn verwerkt maar de activiteiten hier niet op waren gericht. De informatie die binnen het LIMC is verwerkt heeft een maximale rubricering van departementaal vertrouwelijk. In het Defensiebeveiligingsbeleid (DBB) gelden hiervoor de normen van het te beschermen belang niveau 4. Het onderzoekteam heeft diverse documenten en bestanden opgevraagd en ontvangen waarop nader onderzoek is uitgevoerd.

Op 20 november 2020 hebben de afdeling systeemtoezicht van de Autoriteit Persoonsgegevens (AP) en de FG Defensie telefonisch afgestemd. De FG heeft de AP nader geïnformeerd over het ingestelde onderzoek naar de activiteiten van het LIMC.

---

[2] Kamerstukken II 2020/21, 32761 nr. 175. Verwerking en bescherming persoonsgegevens.

[3] Zie artikel 4, aanhef en onder 1, Avg: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.

Op verzoek van de Tweede Kamer heeft de minister van Defensie op 27 november 2020 in een brief[4] medegedeeld dat de FG Defensie een onafhankelijk onderzoek heeft ingesteld en dat in afwachting van de uitkomsten hiervan is besloten om de activiteiten van het LIMC voor wat betreft het verzamelen en analyseren van informatie stil te zetten. In de brief heeft de minister ook een eerste schriftelijke reactie op de activiteiten van het LIMC gegeven.

1.3 Doelstelling

Doelstelling van dit onderzoek is vaststellen in hoeverre de Avg, andere Unierechtelijke of lidstaatrechtelijke gegevensbeschermingsbepalingen en het beleid met betrekking tot de bescherming van persoonsgegevens zijn nageleefd binnen het ministerie van Defensie in het kader van de door het LIMC uitgevoerde activiteiten. De FG rapporteert hierover aan de verwerkingsverantwoordelijke en de Avg-beheerder en treedt op als contactpunt voor de AP als externe toezichthouder.

1.4 Onderzoeksvragen

Centrale onderzoeksvraag

Heeft het ministerie van Defensie in het kader van de door de experimenteeromgeving LIMC uitgevoerde activiteiten gehandeld in overeenstemming met de Avg, de Uitvoeringswet Avg (UAvg) en de Regeling Avg Defensie?

Deelvragen

Om antwoord te kunnen geven op de centrale onderzoeksvraag zijn de volgende deelvragen opgesteld:

1) Zijn er binnen het ministerie van Defensie in het kader van de door de experimenteeromgeving LIMC uitgevoerde activiteiten persoonsgegevens verwerkt zoals bedoeld in de artikelen 2, 4 lid 1 en lid 2 Avg? Is het verwerken van informatie uit openbaar toegankelijk bronnen in overeenstemming met de Avg beoordeeld, gekwalificeerd en ingericht?
2) Zijn er binnen het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten bijzondere categorieën van persoonsgegevens verwerkt zoals bedoeld in artikel 9 Avg? Bijvoorbeeld gegevens betreffende de gezondheid en gegevens betreffende politieke, religieuze of levensbeschouwelijke overtuiging?
3) Indien er binnen het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten verwerkingen van persoonsgegevens hebben plaatsgevonden, met welk welbepaald en omschreven doel hebben de minister van Defensie en de Commandant Landstrijdkrachten deze persoonsgegevens verwerkt en konden de verwerkingen op een rechtmatige grondslag zoals omschreven in de artikelen 6 en 9 Avg worden gebaseerd?
4) Vast te stellen of en zo ja welke personen onder het gezag of in opdracht van het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten persoonsgegevens

[4] Kamerstukken II 2020/21, 32761, nr. 175. Verwerking en bescherming persoonsgegevens.

hebben verwerkt of waar persoonsgegevens aan zijn verstrekt en op welke wijze de logging, autorisatie en toegang tot geautomatiseerde systemen en gegevensbronnen was ingericht. En tevens vast te stellen of het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde activiteiten aan personen of instanties buiten het ministerie van Defensie persoonsgegevens heeft verstrekt en zo ja, met welk doel dat is gebeurd.

5) Diende het ministerie van Defensie in het kader van door de experimenteeromgeving LIMC uitgevoerde verwerkingsactiviteiten een melding op te nemen in het Avg verwerkingenregister Defensie en zo ja, is deze melding gedaan?

6) Was vooraf voor het ministerie van Defensie met het oog op de door de experimenteeromgeving LIMC uit te voeren activiteiten het uitvoeren van een gegevensbeschermingseffectbeoordeling (DPIA) op het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens zoals bedoeld in artikel 35 Avg vereist en zo ja, is er een DPIA uitgevoerd?

7) Welke technische en organisatorische maatregelen zijn door het ministerie van Defensie getroffen ter beveiliging van de in het kader van de door de experimenteeromgeving LIMC uitgevoerde activiteiten verwerkte (persoons)gegevens, zoals bedoeld in artikel 32 Avg en zoals uitgewerkt in het Defensiebeveiligingsbeleid (DBB)?

1.5 Methode van onderzoek

Naast de toezichtbezoeken op locatie heeft het onderzoeksteam een documentenanalyse verricht, een enquête uitgevoerd en interviews gehouden.

Documentenanalyse

In bijlage VII is het overzicht met documenten opgenomen.

Enquête

De enquête is uitgezet bij 151 personen die gedurende een bepaalde periode werkzaamheden hebben verricht voor het LIMC. De namenlijst is verstrekt door de huidige, *acting* chef-staf van het LIMC. De vragen van de enquête zijn opgenomen in bijlage II. Het onderzoek richt zich op de feitelijke gebeurtenissen bij het LIMC en niet op het persoonlijk functioneren van de medewerker. 106 personen hebben op de enquête gereageerd, een respons van 70%. Drie personen geven aan dat zij geen werkzaamheden hebben verricht voor het LIMC.

Interviews

Van 4 tot en met 25 februari 2021 zijn twintig semigestructureerde interviews gehouden. Zestien interviews zijn in verband met de coronamaatregelen via Microsoft Teams gevoerd, vier interviews hebben, met inachtneming van de coronaregels, op de werklocatie van de geïnterviewden plaatsgevonden. De geïnterviewden hebben vooraf een interviewprotocol ontvangen en de via Microsoft Teams geïnterviewde personen hebben achteraf een verslag op hoofdlijnen ter verificatie ontvangen.

1.6 Afbakening

Het onderzoek richt zich op de activiteiten van het LIMC in de periode vanaf de oprichting op 23 maart 2020 tot en met 27 november 2020. Op 27 november heeft

de minister van Defensie besloten de activiteiten van het LIMC voor wat het verzamelen en analyseren van informatie betreft stil te zetten.

Het onderzoek richt zich op de vraag of de activiteiten die door LIMC in deze periode zijn uitgevoerd in overeenstemming waren met de (U)Avg en Regeling Avg Defensie. De FG formuleert daarover conclusies en, indien de bevindingen daartoe aanleiding geven, aanbevelingen. Het onderzoek richt zich niet op de bredere ontwikkelingen op het gebied van informatie gestuurd optreden binnen de krijgsmacht, bij andere defensieonderdelen of CD&E (concept *development & experimentation*) projecten buiten het LIMC.

1.7 Rapportopbouw

In hoofdstuk twee is het toetsingskader beschreven op basis waarvan de bevindingen in hoofdstuk drie zijn beoordeeld. Het toetsingskader bestaat naast privaat- en publiekrechtelijke kaders, zoals de Avg en hierop gebaseerde regelgeving, uit defensiekaders zoals de Regeling Avg Defensie en het DBB. Het rapport wordt afgesloten met hoofdstuk vier waarin de conclusies en aanbevelingen staan verwoord.

2 Toetsingskader

Voordat wordt toegekomen aan een inhoudelijke beoordeling van de activiteiten en de verwerking van persoonsgegevens binnen het LIMC, is allereerst van belang om vast te stellen of en zo ja, in hoeverre de Avg (en de Uavg) van toepassing is.

Vaststaat dat, voor zover het gaat om verwerking van persoonsgegevens, de verwerkingsactiviteiten binnen het LIMC, binnen het territoriaal toepassingsgebied van de Avg (en de Uavg) vallen. De verwerkingsactiviteiten vinden immers plaats in Nederland onder beheer van het ministerie van Defensie, dat is gevestigd in Nederland.[5]

Van belang voor dit onderzoek is met name de vraag of de activiteiten en de verwerking van persoonsgegevens binnen het LIMC ook binnen het materiële toepassingsgebied van de Avg en de Uavg vallen. Kort gezegd: verwerkt het LIMC persoonsgegevens en zo ja, is de Avg hierop van (overeenkomstige) toepassing of zijn de gegevensverwerkingen uitgezonderd van het materieel toepassingsgebied van de verordening, bijvoorbeeld op grond van het bepaalde in artikel 2 Avg en de artikelen 2 en 3 Uavg.

Daarna volgt in dit hoofdstuk een toelichting op enkele beginselen van de Avg. Allereerst wordt rechtmatigheid (de wettelijke grondslag) toegelicht, gevolgd door doelbinding, noodzakelijkheid, juistheid, passende technische en organisatorische maatregelen en verantwoording. Het hoofdstuk wordt afgesloten met een toelichting op bijzondere en strafrechtelijke persoonsgegevens.

2.1 Materieel toepassingsgebied

De Avg is materieel van toepassing op de geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.[6]

2.1.1 *Persoonsgegevens*

Een persoonsgegeven is alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[7] Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct (bijvoorbeeld aan de hand van een naam, adres, telefoonnummer), of indirect (bijvoorbeeld met behulp van een klantnummer, autokenteken) kan worden geïdentificeerd.[8] Van een persoonsgegeven is aldus snel sprake.

Voor de vraag of sprake is van identificeerbaarheid moet worden gekeken naar alle middelen waarvan mag worden aangenomen dat zij redelijkerwijs door degene die voor de verwerking verantwoordelijk is, dan wel door derden in te zetten zijn, om de persoon te identificeren. Daarbij moet rekening worden gehouden met alle objectieve factoren, zoals de kosten van en de tijd benodigd voor identificatie, met

---

[5] Zie artikel 3, eerste lid Avg respectievelijk artikel 4 eerste lid UAvg.
[6] Zie artikel 2, eerste lid, Avg.
[7] Zie artikel 4, aanhef en onder 1, Avg.
[8] In de definitie van het begrip persoonsgegeven in de Avg wordt gesproken over identificatie "met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon".

inachtneming van de beschikbare technologie op het tijdstip van verwerking maar ook de technologische ontwikkelingen in de nabije toekomst (denk aan de toenemende rekenkracht van computers en het groeiende aantal beschikbare hulpmiddelen).[9]

De Avg is niet van toepassing op gegevens die zodanig anoniem zijn (gemaakt) dat de persoon waarop ze betrekking hebben niet (meer) zonder onredelijke inspanning identificeerbaar is. In dat geval is er, met andere woorden, geen sprake van verwerking van persoonsgegevens meer. Het anonimiseren op zichzelf is overigens al een verwerking van persoonsgegevens.

2.1.2 *(Geautomatiseerde en/of handmatige) verwerking*

Een verwerking is iedere bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Dit betreft een ruim begrip. Als voorbeelden noemt artikel 4, tweede lid, Avg onder meer het verzamelen, opslaan, bijwerken, raadplegen en doorzenden van persoonsgegevens.[10] Ook het enkel opzoeken en/of analyseren van data, betreft een verwerking in de zin van de Avg.

Daarnaast is van belang, voor de materiële toepasselijkheid van de Avg, of de verwerking, waaronder dus het raadplegen, van persoonsgegevens (gedeeltelijke)[11] geautomatiseerd (lees: met behulp van computers of soortgelijke digitale middelen)[12] plaatsvindt, danwel een handmatige verwerking van persoonsgegevens die in een bestand[13] zijn opgenomen of die bestemd zijn om daarin te worden opgenomen, betreft. Alleen in dat geval is de Avg (en de Uavg) van toepassing.[14] Zie overweging 27 van de considerans van de voormalige Richtlijn 95/46/EG[15] die dezelfde bepaling kende: "Overwegende dat de bescherming van personen zowel op automatische als op niet-automatische verwerking van toepassing is; dat de reikwijdte van deze bescherming in feite niet afhankelijk mag zijn van de gebruikte technieken, omdat zulks ernstig gevaar voor ontduiking zou opleveren; dat niettemin wat de niet-automatische verwerking betreft alleen bestanden en geen ongestructureerde dossiers onder de richtlijn vallen (...)". [16]

---

[9] Overweging 26 van de considerans van de Avg.

[10] Zie voor de volledige opsomming artikel 4, onder 2, Avg: '"verwerking: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.'

[11] Er is sprake van een 'gedeeltelijke geautomatiseerde verwerking' als bij een onderdeel van de verwerking niet alleen gebruik gemaakt wordt van computers, smartphones, tablets, servers, databases et cetera, maar ook gebruik gemaakt wordt van andere middelen.

[12] Zie Afdeling Bestuursrechtspraak van de Raad van State ("ABRvS") 31 december 2014, ECLI:NL:RVS:2014:4753, rov. 6.2.

[13] Zie artikel 4, onder 6, Avg: „bestand": elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid."

[14] Zie artikel 2, eerste lid, Avg.

[15] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

[16] Zie in dat verband tevens ABRvS 16 juli 2014, ECLI:NL:RVS:2014:2594, rov. 5.5: "Gezien het vorenstaande volgt uit de bewoordingen van artikel 2, eerste lid, van de Wbp en artikel 3, eerste lid, van de Privacyrichtlijn, gelezen in samenhang met de overwegingen van de considerans bij die richtlijn, dat

Een aantal voorbeelden van (gedeeltelijk) geautomatiseerde verwerkingen zijn in de toelichting bij de Wet bescherming persoonsgegevens ("Wbp") opgesomd, waaronder het uitvoeren van zoekopdrachten met behulp van daartoe geschreven programma's. Zie Kamerstukken II 1997/98, 25 892, nr. 3, p. 69: "Hieruit vloeit voort dat iedere «losse» verwerking van geheel of gedeeltelijk geautomatiseerde gegevens onder het bereik van dit wetsvoorstel valt. Gedacht kan worden aan het opslaan van een persoonsgegeven op een (optisch-)magnetische gegevensdrager als de tekstverwerker of een chipcard. Ook de verwerking van persoonsgegevens voor datamining of de uitvoering van bepaalde zoekopdrachten (*query's*) met behulp van daartoe geschreven programma's, al dan niet verricht door de verantwoordelijke zelf, valt onder de algemene normering van gegevensverwerking."

2.1.3 *Big Data*

Big Data is een wijdverspreide en veelgebruikte term. Toch bestaat er geen breed gedeelde definitie van *Big Data*, zo constateerde de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) in haar rapport 'Big Data in een vrije en veilige samenleving'.

De WRR benoemt in haar rapport drie hoofdkenmerken van *Big Data*:

- Data: grote hoeveelheden gestructureerde of ongestructureerde gegevens of een combinatie van beide uit verschillende databronnen.
- Data-gedreven analyse: er wordt gezocht naar patronen in de data zonder vooraf opgestelde hypotheses. Analyses zijn vooral gericht op het heden (*realtimeanalyses/nowcasting*) en de toekomst (*predictive analyses/forecasting*).
- Gebruik: data uit het ene domein wordt gebruikt voor beslissingen in een ander domein met ontschotting van domeinen als gevolg. *Actionable knowledge*: conclusies op geaggregeerd niveau kunnen worden toegepast voor beslissingen op groeps- of individueel niveau (persoon of object).

2.1.4 *Uitzonderingen (U)Avg: krijgsmacht*

De Avg en UAvg zijn vrijwel volledig van overeenkomstige toepassing verklaard op de verwerkingen van persoonsgegevens in het kader van de activiteiten van de krijgsmacht. Uitgezonderd zijn verwerkingen van persoonsgegevens door de krijgsmacht:

- indien de minister van Defensie daartoe heeft beslist;
- met het oog op de inzet of het ter beschikking stellen van de krijgsmacht ter uitvoering van de in artikel 97 van de Grondwet omschreven taken voor zover dat noodzakelijk is voor de vervulling van het mandaat en de bescherming van de (internationale) troepenmacht.

Daarnaast bestaat er voor Defensie een uitzondering, uit hoofde van artikel 3, derde lid, onder a en b, UAvg, indien de Wet op de inlichtingen- en veiligheidsdiensten 2017 van toepassing is op de verwerking van persoonsgegevens.

Tevens uitgezonderd is, de verwerking van persoonsgegevens door de bevoegde autoriteiten, waaronder de Koninklijke Marechaussee, met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

---

het in geval van geautomatiseerde verwerking van persoonsgegevens niet van belang is of deze gegevens een bestand als bedoeld in artikel 1, aanhef en onder c, van de Wbp, vormen. [...]."

Juridische onderbouwing

De gedetailleerde juridische onderbouwing is als volgt:

- Uitgezonderd van het materiële toepassingsgebied van de Avg, zijn, op grond van artikel 2, tweede lid, onder a en b, Avg, de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen; en door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, Verdrag betreffende de Europese Unie ("VEU") vallen.
- Tevens uitgezonderd is, de verwerking van persoonsgegevens door de bevoegde autoriteiten, waaronder de Koninklijke Marechaussee, met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid (zie in dat verband artikel 2, tweede lid, onder d, Avg).[17]
- De Nederlandse wetgever heeft in artikel 3 UAvg een nadere uitwerking gegeven aan de reikwijdte van deze uitzonderingen uit artikel 2, tweede lid, Avg. Deze nadere uitwerking van de reikwijdte van de uitzondering uit artikel 2, tweede lid, Avg, is door de Nederlandse wetgever aangebracht om tegemoet te komen aan de regelingsopdracht van artikel 10, tweede en derde lid, van de Grondwet. Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 9 en 13-14:

  "[D]e nationale wetgever [dient,] [niet alleen bij] het invullen van de grondwettelijke opdracht via Europese regels[, maar ook in diverse andere opzichten] het Nederlandse constitutionele perspectief [te behartigen]. De regering wijst erop dat gegevensbescherming een belangrijke rol speelt op de gebieden die geheel of gedeeltelijk aan het Unierecht zijn onttrokken. Te denken valt met name aan de verwerking van persoonsgegevens met het oog op de nationale veiligheid door inlichtingen- en veiligheidsdiensten [en door Defensie.[18]] De wetgever kan op dat terrein nog in belangrijke mate zelfstandig invulling geven aan de regelingsopdracht van artikel 10, tweede en derde lid, van de Grondwet." (tekst tussen blokhaken toegevoegd)

  Zie ook *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 13 en 14:

  "In artikel 3, tweede lid, onder eerste streepje, van de richtlijn is bepaald dat, ook in dat geval echter verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat – waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van staatsveiligheid – en de activiteiten van de Staat op strafrechtelijk gebied, niet onder het bereik van de richtlijn vallen. [...] Deze beperking hangt samen met de grondslag van de richtlijn, te wetende harmonisatie met het oog op de totstandkoming van de interne markt. De Lidstaten blijven vrij de regelgeving voor het overige naar eigen inzicht in te richten, zij het binnen de grenzen van het Verdrag inzake gegevensbescherming voor zover zij dit hebben bekrachtigd. Het wetsvoorstel behelst de keuze af te zien van het onderscheid of een vorm

[17] Zie artikel 1, onder a, Wet politiegegevens jo. artikel 4 Politiewet 2012.
[18] Daarbij opgemerkt dat er in de Uitvoeringswet voor is gekozen om gegevensverwerking door de krijgsmacht onder de werkingssfeer van deze wet te brengen en de verordening van overeenkomstige toepassing te verklaren, met dien verstande dat de minister van Defensie in bepaalde gevallen hiervan kan afwijken.

van gegevensverwerking al dan niet onder het communautaire recht valt. Dit vermijdt onnodige vragen over de precieze reikwijdte van het zich voortdurend uitbreidende communautaire recht, alsmede vragen naar de rechtvaardiging waarom een bepaald rechtsgebied dat onder het communautaire recht valt, anders wordt geregeld dan een rechtsgebied waarbij dat (nog) niet het geval is."

- Op grond van artikel 3, eerste lid, onder a en b, en het tweede lid, UAvg zijn de UAvg en de Avg (en de daarop berustende bepalingen) mede van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen; en op verwerkingen door de krijgsmacht bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, van het VEU vallen. De Avg en de UAvg zijn daarmee dus vrijwel volledig van overeenkomstige toepassing verklaard op de verwerkingen van persoonsgegevens in het kader van de activiteiten van de krijgsmacht.
- Op het voorgaande bestaat, uit hoofde van artikel 3, derde lid, onder a, UAvg, alleen een uitzondering indien onze minister van Defensie heeft beslist (bepaalde) verwerkingen van persoonsgegevens door de krijgsmacht, met het oog op de inzet of het ter beschikking stellen van de krijgsmacht ter uitvoering van de in artikel 97 van de Grondwet omschreven taken uit te zonderen. De geldende uitzonderingen zijn door de minister van Defensie opgenomen in de Regeling Gegevensbescherming Militaire Operaties ("RGMO"). Aangezien overeenkomstige toepassing van de Avg het uitgangspunt is, zien de uitzonderingen in de RGMO alleen op de taakuitvoering voor zover dat noodzakelijk is voor de vervulling van het mandaat en de bescherming van de (internationale) troepenmacht. Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 90-91:

  "Zoals hierboven aangegeven zijn gegevensverwerkingen in het kader van inzet van de krijgsmacht op basis van artikel 2 van de verordening uitgesloten van de reikwijdte van de verordening. Het is desalniettemin wenselijk dat op verwerkingen door de krijgsmacht ten behoeve van de uitvoering van haar taken, bedoeld in artikel 97 van de Grondwet, de Uitvoeringswet en de verordening in beginsel wel van toepassing onderscheidenlijk van overeenkomstige toepassing zijn. Hiermee wordt de huidige in de Wbp vervatte lijn (artikel 2, derde lid, van de Wbp)[19] voortgezet dat ook in geval van inzet of het ter beschikking stellen van de krijgsmacht waar mogelijk de algemene beginselen voor de verwerking van persoonsgegevens in acht worden genomen.

---

[19] Zie ook de Memorie van Toelichting bij de voorganger van artikel 3 UAvg; artikel 2, derde lid, Wbp (*Kamerstukken II* 1997/98, 25 892, nr. 3, p. 72): "Het derde lid voorziet in een voorwaardelijke uitzondering voor gegevensverwerkingen door de krijgsmacht in geval van daadwerkelijk operationeel optreden door Nederlandse militairen in het buitenland. Gedacht dient te worden aan de inzet van de krijgsmacht bij internationale crisisbeheersingsoperaties. Hoewel gegevensverwerkingen in dat kader veelal buiten Nederland zullen worden verricht, blijft de minister van Defensie hiervoor verantwoordelijk. Mede gelet op artikel 4 zou de wet zonder nadere voorziening van toepassing zijn. Bij inzet in internationale crises kan evenwel niet altijd worden gevergd dat de wet onverkort wordt toegepast. De omstandigheden waarin de krijgsmacht dan soms moet functioneren laten zulks in bepaalde gevallen niet toe. Om die reden wordt in het derde lid de bevoegdheid toegekend aan de minister van Defensie om te bepalen dat de wet buiten toepassing kan blijven. De minister kan daartoe slechts beslissen indien dit met het oog op de inzet van de krijgsmacht ter handhaving of bevordering van de internationale rechtsorde nodig is. Met deze laatste formulering is aangesloten bij het nieuwe artikel 97 van het recent ingediende voorstel van Rijkswet tot wijziging van de bepalingen van de Grondwet inzake de verdediging. Ten slotte is bepaald dat de Registratiekamer van de beslissing van de minister – zo nodig achteraf doch zo spoedig mogelijk – in kennis dient te worden gesteld. Deze voorziening is er op gericht om een adequate controle op de toepassing van de wet mogelijk te maken. Met het oog daarop zal de beslissing van de minister om de wet buiten toepassing te laten, van een adequate motivering moeten zijn voorzien."

Er moet evenwel een mogelijkheid zijn om af te wijken, omdat bij inzet in internationale militaire operaties niet altijd kan worden gevergd dat alle bepalingen onverkort worden 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." (tekst tussen blokhaken toegevoegd) Vgl. ook Nota van Toelichting bij de Regeling Gegevensbescherming Militaire Operaties (*Stb.* 2018, 28293).

- Daarnaast bestaat er voor Defensie een uitzondering, uit hoofde van artikel 3, derde lid, onder a en b, UAvg[20], indien de Wet op de inlichtingen- en veiligheidsdiensten 2017 van toepassing is op de verwerking van persoonsgegevens.

2.1.5 *Uitzonderingen (U)Avg: persoonlijke, huishoudelijke & journalistieke doeleinden*

De uitzonderingen voor persoonlijke, huishoudelijke en journalistieke doeleinden zijn op de verwerking bij het LIMC niet van toepassing.

De gedetailleerde juridische onderbouwing is als volgt:

- Uitzondering (op de toepasselijkheid van de Avg en de UAvg) uit artikel 2, tweede lid, onder c, Avg inzake de verwerkingen van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit,[21] is niet relevant voor het gebruik door het LIMC. Dit omdat het bij het LIMC niet gaat om verwerkingen door een natuurlijk persoon, maar door ambtenaren van de krijgsmacht die handelen onder gezag en verantwoordelijkheid van de Minister van Defensie. De verwerking heeft dus niet een louter persoonlijk of huishoudelijk karakter, maar houdt verband met een beroepsactiviteit.[22]
- De uitzondering inzake de vrijheid van meningsuiting, zoals voortvloeit uit artikel 85 Avg jo. artikel 43 UAvg,[23] is hier niet relevant. Deze uitzondering geldt immers uitsluitend voor gegevensverwerkingen voor journalistieke,[24] artistieke of literaire doeleinden en niet voor de onderhavige verwerkingen door de overheid. Dit omdat er geen sprake is van journalistiek, zijnde een verwerking die als enig doel heeft de bekendmaking aan het publiek van informatie, meningen of ideeën, noch van artistieke of literaire doeleinden die worden nagestreefd.

---

[20] Zie in dat verband ook artikel 2, tweede lid, onder a, Avg.

[21] Zie artikel 2, tweede lid, onder c, Avg. Deze uitzondering dient volgens de Autoriteit Persoonsgegevens maar ook het Hof van Justitie van de Europese Unie ("HvJ EU"), zoals onder meer blijkt uit het arrest van 11 december 2014 van het HvJ EU (ECLI:EU:C:2014:2428, C-212/13, (*Reynes*)), strikt te worden uitgelegd. Zie de website van de Autoriteit Persoonsgegevens (raadpleegbaar via: https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/persoonsgegevens-op-internet#wat-is-de-uitzondering-voor-persoonlijk-of-huishoudelijk-gebruik-6433).

[22] Zie in dat verband overweging 18 van de considerans van de Avg.

[23] Zie ook overweging 153 bij de considerans van de Avg.

[24] In dit verband zijn de volgende uitspraken van belang: HvJ EU van 16 december 2008, ECLI:EU:C:2008:727 (*Satamedia*), par. 57 e.v.; EHRM 27 juni 2017, ECLI:CE:ECHR:2017:0627JUD000093113, nr. 931/13 (*Satamedia*); HvJ EU, 14 februari 2019, ECLI:EU:C:2019:122, nr. C-345/17 (*Buidvids*). Zie verder ook de recente uitspraak Rechtbank Midden-Nederland 23 november 2020, ECLI:NL:RBMNE:2020:5111 (*VoetbalTv*).

2.2 Rechtmatig: wettelijke grondslag

Artikel 5, eerste lid, aanhef en onder a, Avg schrijft voor dat persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is.

Deze eis vindt in feite zijn uitwerking in een groot deel van de overige privacy-eisen, waaronder artikel 6, eerste lid, Avg. Dit artikel bepaalt dat een verwerking van persoonsgegevens enkel is toegestaan voor zover daarvoor een zogenoemde 'wettelijke grondslag'[25],bestaat. De algemene wettelijke grondslagen van artikel 6, eerste lid, Avg luiden als volgt:

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

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.

Voor de verwerkingen binnen het LIMC kan gebruik gemaakt worden van de verwerkingsgrondslagen van artikel 6, eerste lid, onder e, Avg (vervulling van een taak van algemeen belang) en artikel 6, eerste lid, onder c, Avg (wettelijke verplichting). De grondslag moet te vinden zijn in het recht van de Europese Unie of het recht van een lidstaat. Het is immers aan de wetgever om de rechtsgrond voor de persoonsgegevensverwerkingen door overheidsinstanties te creëren.[26]

Daarbij wel de opmerking dat het hebben van een wettelijke grondslag voor een publieke taak, volgens de wetgever, niet altijd betekent dat de wettelijke grondslag voor de gegevensverwerking gegeven is. Dit plaatst de wetgever in het verlengde van het daarover opgemerkte in artikel 8, tweede lid, EVRM. Zie in dat verband de *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 35-36 (inzake de 'gewone grondslag' in de zin van artikel 6 Avg):

"[...] Uit de eis dat een inmenging in de uitoefening van het recht op respect voor het privéleven als bedoeld in artikel 8 van het EVRM moet zijn voorzien bij wet («*in accordance with the law*») vloeit voort dat die inmenging moet berusten op een naar behoren bekendgemaakt wettelijk voorschrift waaruit de burger met voldoende precisie kan opmaken welke op zijn privéleven betrekking hebbende gegevens met het oog op de vervulling van een bepaalde overheidstaak kunnen worden verzameld en vastgelegd, en onder welke voorwaarden die gegevens met dat doel kunnen

[25] Als bedoeld in artikel 6, eerste lid, Avg.
[26] Zie overweging 47 van de considerans van de Avg.

worden bewerkt, bewaard en gebruikt. Vereist is dus een voldoende precieze wettelijke grondslag. Dat betekent dat bijvoorbeeld de algemene taakstelling van een overheidsdienst niet in alle gevallen kan dienen als rechtsgrond voor gegevensverwerking.[17]"

De verwerkingen van persoonsgegevens door de overheid binnen het LIMC dienen zodoende, zoals volgt uit artikel 8 tweede lid EVRM, voldoende duidelijk voort te vloeien uit een naar behoren bekend gemaakt en voldoende precies wettelijk voorschrift.

2.2.1 *De publieke taken van de krijgsmacht*

De publieke taken van de krijgsmacht kunnen, zoals voortvloeit uit artikel 97, eerste lid, Grondwet, liggen in de volgende doelen: de verdediging van het Koninkrijk en de bondgenootschappelijke verdediging; de handhaving en de bevordering van de internationale rechtsorde; en de bescherming van belangen van het Koninkrijk.

In de Defensienota uit 2018, worden deze taken op de volgende wijze uitgewerkt:[27]

"1 Bescherming van het eigen en bondgenootschappelijke grondgebied, inclusief het Caribisch deel van het Koninkrijk.
2 Bescherming en bevordering van de internationale rechtsorde en stabiliteit.
3 Ondersteuning van civiele autoriteiten bij rechtshandhaving, rampenbestrijding en humanitaire hulp, zowel nationaal als internationaal."

Deze taken worden, zoals blijkt uit artikel 97, tweede lid, Grondwet, door de regering toebedeeld. De regering bepaalt of, en zo ja hoe, de krijgsmacht voor deze doelen uiteindelijk wordt ingezet.[28] Uit artikel 97 Grondwet vloeit als zodanig, geen - zelfstandig werkende - taak of bevoegdheid voor de krijgsmacht voor nationale inzet, voort[29].

Inzet van de krijgsmacht voor nationale taken is alleen mogelijk voor zover deze taken zijn vastgelegd in wet- en regelgeving; in geval van structurele ondersteuning van civiel gezag, zijn vastgelegd in convenanten of arrangementen; of op basis van bijstand of Militaire Steunverlening in het Openbaar Belang ("MSOB")[30].
Voor zover structurele taken van de krijgsmacht zijn vastgelegd in wet- en regelgeving, vloeit uit die wet- en regelgeving voort in hoeverre een verwerking van persoonsgegevens in dat kader mogelijk is.

Een voorbeeld van een structurele taak zijn de (politie)taken, zoals vastgelegd in artikel 4 Politiewet 2012, van de Koninklijke Marechaussee en de taak van de krijgsmacht die is belegd in de Rijkswet geweldgebruik bewakers militaire objecten. Deze wet geeft de krijgsmacht bepaalde geweldsbevoegdheden in de uitoefening van de wettelijke bewakings- en beveiligingstaak.

---

[27] Raadpleegbaar via https://www.defensie.nl/downloads/beleidsnota-s/2018/03/26/defensienota-2018.
[28] Zie *Kamerstukken II* 1997/98, 25 367 (R 1593), nr. 3, p. 3.
[29] Zie artikel 97, tweede lid, Grondwet. Daaruit blijkt dat de regering het oppergezag heeft over de krijgsmacht. Met andere woorden, de (wettelijk) vastgelegde bevoegdheid om de krijgsmacht in te zetten. Zie daarover P. A. L., Ducheine en G. L. C. van den Bosch, 'Staatsrecht en krijgsmacht', in: M. D. Fink (editor), *Inleiding militair recht*. Den Haag: Nederlandse Defensie Academie 2014 (derde druk), p. 11-28. *Kamerstukken II* 1997/98, 25 367 (R 1593), nr. 3, p. 3.
[30] Zie de Regeling inzake militaire steunverlening in het openbaar belang.

Bij (niet-structurele) nationale inzet op basis van bijstand (op basis van bijvoorbeeld artikel 58 van de Politiewet 2012; of artikel 20 van de Wet Veiligheidsregio's) of MSOB, wordt de krijgsmacht ingezet onder aansturing en verantwoordelijkheid van civiel gezag, zoals de officier van justitie of de burgemeester. Daarbij oefent de krijgsmacht niet altijd eigen publieke taken en bevoegdheden uit, maar taken en bevoegdheden van het ondersteunde civiele gezag (en is – in het verlengde daarvan – geen verwerkingsverantwoordelijke). Ter uitoefening van die taken en bevoegdheden mag de krijgsmacht persoonsgegevens verwerken, voor zover het civiele gezag, als verwerkingsverantwoordelijke, de krijgsmacht daartoe de opdracht heeft gegeven en deze verwerking noodzakelijk is voor de vervulling van een taak of onderdeel is van een bevoegdheid van het civiele gezag.

2.3 Doelbinding

Persoonsgegevens moeten, op grond van artikel 5, aanhef en onder b, Avg, voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en mogen niet verder op een met die doeleinden onverenigbare wijze worden verwerkt (het doelbindingsbeginsel).

De doeleinden waarvoor persoonsgegevens worden verwerkt dienen, zoals is verduidelijkt in overweging 39 van de considerans van de Avg, te zijn vastgelegd wanneer de persoonsgegevens worden verzameld. De doeleinden dienen expliciet en gerechtvaardigd te zijn.

Een verwerking van persoonsgegevens vindt plaats voor een gerechtvaardigd doeleinde, indien deze kan worden gebaseerd op een grondslag als bedoeld in artikel 6 Avg en het doeleinde in overeenstemming is met toepasselijke wet- en regelgeving. Voor verwerkingen die worden gebaseerd op artikel 6, eerste lid, onder e, Avg (de verwerkingen zijn noodzakelijk zijn voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag), geldt dat het doel van de verwerking in de wetgeving wordt vastgesteld (artikel 6, derde lid, Avg).

Een verwerking van deze verzamelde persoonsgegevens kan plaatsvinden voor een ander doeleinde dan waarvoor deze persoonsgegevens oorspronkelijk zijn verzameld (een 'verdere verwerking') indien het doeleinde van de verdere verwerking verenigbaar is met het oorspronkelijke doel van de verwerking van de gegevens. Of een verdere verwerking, voor een ander doel, verenigbaar is wordt bepaald aan de hand van de criteria genoemd in artikel 6, vierde lid, Avg. Als er op basis daarvan wordt vastgesteld dat er geen sprake is van een verenigbare verdere verwerking, is deze verwerking alleen toegestaan voor zover de verwerking berust op (i) toestemming, (ii) een Europese of nationale wettelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van een in artikel 23, eerste lid, Avg bedoelde doeleinden (nationale veiligheid, landsverdediging, openbare veiligheid).

Aan de hand van de volgende criteria wordt bepaald of verdere verwerking verenigbaar is met de verzameldoeleinden:

- Het verband tussen de doeleinden waarvoor de gegevens zijn verzameld en de doeleinden van de verdere verwerking;
- 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);
- De aard van de gegevens;
- De mogelijke gevolgen van de voorgenomen verdere verwerking voor betrokkenen; en

- Het bestaan van passende waarborgen, zoals pseudonimisering.

Van belang is verder het "vermoeden van verenigbaarheid" als bedoeld in artikel 5, eerste lid, onder b, van de Avg. Op grond daarvan wordt een verdere verwerking met het oog op wetenschappelijk onderzoek niet als onverenigbaar beschouwd.[31]

Indien sprake is van een verenigbare verdere verwerking, dan is bij een interne verdere verwerking (door dezelfde verwerkingsverantwoordelijke) geen afzonderlijke wettelijke grondslag als bedoeld in artikel 6, eerste lid, Avg vereist. Bij een externe verdere verwerking (door een andere verwerkingsverantwoordelijke) dient de verwerkingsverantwoordelijke over een afzonderlijke wettelijke grondslag als bedoeld in artikel 6, eerste lid, Avg te beschikken. Zie *Kamerstukken II* 2018/19, 34 851, nr. 3, p. 38[32].

2.4 Noodzakelijkheid

Uit het noodzakelijkheidsbeginsel van artikel 5, eerste lid, aanhef en onder c, Avg, ook wel aangeduid als 'het beginsel van dataminimalisatie', volgt dat de privacy inbreuk die gepaard gaat met verwerkingen van het LIMC noodzakelijk moet zijn voor het doel waarvoor het LIMC wordt ingezet ('proportionaliteit').

Daarnaast mag de verwerkingsverantwoordelijke slechts overgaan tot het verwerken van (strafrechtelijke of bijzondere) persoonsgegevens indien het onderzoeksdoel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit').

Het noodzakelijkheidsbeginsel heeft tot slot ook gevolgen voor de toegang tot, de omvang en de aard van de persoonsgegevens die ten behoeve van het LIMC door de verwerkingsverantwoordelijke mogen worden verwerkt. De persoonsgegevens dienen toereikend en ter zake dienend te zijn en moeten beperkt blijven tot het strikt noodzakelijke. Kort en goed houdt dit in dat de verwerkingsverantwoordelijke enkel '*need to know*'-informatie mag verwerken, in plaats van '*nice to know*'-informatie.

Het noodzakelijkheidsbeginsel zal ook technisch en organisatorisch door ontwerp en standaardinstellingen binnen het LIMC moeten worden geborgd, zodat kan worden voldaan aan de beginselen van *privacy by design and default* uit artikel 25 Avg. In hoeverre en op welke manier de verwerkingsverantwoordelijke uitvoering dient te geven aan deze beginselen, vormt de uitkomst van een afweging van verschillende factoren.[33]

De verplichting uit artikel 25 Avg is het best te begrijpen als een zorgplicht van de verwerkingsverantwoordelijke om een zo beperkt mogelijke inbreuk op de persoonlijke levenssfeer te maken bij de verwerking van persoonsgegevens.[34]

---

[31] Zie ook EDPB, 'Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak', 21 april 2020 (raadpleegbaar via, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_nl.pdf).

[32] Deze opmerking in de memorie van toelichting is toegevoegd naar aanleiding van het wetgevingsadvies van de Afdeling advisering van de Raad van State (*Kamerstukken II* 2017/18, 34 851, nr. 4, p. 36-38).

[33] Die factoren zijn (onder meer) de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context en het doel van de verwerking en de risico's (waarschijnlijkheid en ernst) voor de rechten en vrijheden van de betrokkenen. Zie voor een concretisering hiervan de overwegingen 75 en 76 van de considerans van de Avg.

[34] Deze zorgplicht zal in verschillende contexten geconcretiseerd moeten worden, maar verschillende elementen worden al expliciet in overweging 78 van de considerans van de Avg genoemd.

2.5 Juistheid

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 op grond van artikel 5, eerste lid, onderdeel d, Avg de nodige maatregelen treffen om ervoor te zorgen dat de persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn.

Voorts dient de verwerkingsverantwoordelijkheden persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren.

2.6 Passende technische en organisatorische maatregelen

De Avg schrijft in artikel 32 voor dat "passende technische en organisatorische maatregelen" worden getroffen ter beveiliging van de verwerking.

Dit zijn twee open normen. Om te bepalen wat voor het LIMC een passende beveiliging is om het doel van artikel 32 Avg te bereiken, zijn de normen en maatregelen van het Defensie beveiligingsbeleid gehanteerd.

2.6.1 *Defensiebeveiligingsbeleid*

Het ministerie van Defensie levert een belangrijke bijdrage ten behoeve van de bevordering van vrede en veiligheid in de wereld. Personeel, informatie en materieel zijn van wezenlijk belang om een effectieve uitvoering van taken in dit kader te kunnen garanderen. Een ieder moet bij de taakuitvoering onder alle omstandigheden kunnen vertrouwen op de betrouwbaarheid van de bedrijfsprocessen. Die betrouwbaarheid wordt onder meer gegarandeerd door het treffen van beveiligingsmaatregelen. Het geheel aan personele, fysieke, informatie- en industriebeveiliging wordt integrale beveiliging (*security*) genoemd. Integrale beveiliging is beschreven in het DBB.

Het DBB is ontwikkeld op basis van externe normenkaders en regelgeving zoals NATO- en EU beveiligingsbeleid, civiele beveiligingsnormen zoals NEN-ISO/IEC 27001:2017 en 27002:2017, de Baseline Informatiebeveiliging Overheid (BIO) het Besluit voorschrift informatiebeveiliging rijksdienst (VIR) en het Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere informatie (VIR-BI) et cetera. Alle externe van toepassing zijnde normen en maatregelen zijn geïncorporeerd binnen het DBB en hieraan zijn defensie specifieke normen en maatregelen toegevoegd. Het DBB is daardoor een zwaarder beleidskader dan de Baseline Informatiebeveiliging Overheid. De BIO is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). Met het implementeren van het DBB wordt een beveiligingsniveau bereikt dat tenminste gelijk is aan de BIO maar in de meeste gevallen hoger. Voor het DBB geldt het 'Pas toe of leg uit' principe. Hiermee wordt bedoeld dat Defensie de normen toepast tenzij er expliciet geformuleerde redenen zijn om dat niet te doen.

Niveau van normen en maatregelen
Het niveau van de normen en maatregelen hangt af van de aard van de informatie, het materieel, de goederen en de objecten in relatie tot de specifieke dreiging. Het ministerie van Defensie hanteert daartoe een rubricering- en merking-systeem. Defensie heeft alle te beschermen informatie, materieel, goederen en objecten

ingedeeld in vier categorieën Te Beschermen Belang (TBB, met TBB 1 als strengst te beveiligen categorie).

Bijzondere informatie, rubricering departementaal vertrouwelijk, merking personeelsvertrouwelijk.
Informatie die is voorzien van een rubricering wordt Bijzondere Informatie (BI) genoemd. Ook BI valt, afhankelijk van de hoogte van de rubricering, in een TBB-categorie. Een gerubriceerd document is altijd een TBB, maar een TBB is niet altijd gerubriceerd. Een voorbeeld van een rubricering is DEPARTEMENTAAL VERTROUWELIJK. Kennisname door niet-gerechtigden van de BI kan nadeel toebrengen aan het belang van een of meer ministeries.

Naast rubriceringen kent Defensie merkingen zoals PERSONEELSVERTROUWELIJK.

2.6.2 *Normen LIMC*

Bij het LIMC zijn de normen en maatregelen van TBB niveau 4 als norm gehanteerd. Dit is gebruikelijk voor DEPARTEMENTAAL VERTROUWELIJK gerubriceerde bijzondere informatie of PERSONEELSVERTROUWELIJK gemerkte informatie. Overigens is de merking PERSONEELSVERTROUWELIJK geen synoniem voor persoonsgegevens. Niet alle persoonsgegevens vallen onder deze definitie van de merking bij Defensie.

Onderstaande normen en maatregelen zijn het meest relevant in relatie tot de "veilige verwerking" van persoonsgegevens. Daarnaast zijn enkele beveiligingsnormen geselecteerd waar, binnen het LIMC, specifiek naar is gekeken zoals fysiek Te Beschermen Belangen en informatiedragers. Daarbij is het *need-to-know* en *need-to-be* principe te allen tijde van toepassing. Als het DBB wordt nageleefd wordt voldaan aan het doel van artikel 32 Avg.

2.6.3 *Norm: organisatorische maatregelen*

Geheimhoudingsverklaring
Iedere medewerker (ongeacht het dienstverband) ondertekent een verklaring omtrent de bekendheid met de geheimhoudingsplicht. Deze verklaring is verplicht en eenmalig, en blijft geldig ook na het beëindigen van het dienstverband.

Beveiligingsbriefing
Binnen Defensie zijn verschillende procedures en activiteiten met als doel het beveiligingsbewust maken en houden van medewerkers. Dit onderwerp staat binnen Defensie hoog op de agenda en kent verschillende uitwerkingen bijvoorbeeld:

- initiële, periodieke en jaarlijkse beveiligingsbriefings;
- beveiligingsbewustwording als onderdeel van interne cursussen / opleidingstrajecten;
- digitaal rijbewijs;
- beveiligingsbewustzijnprogramma en -workshops;
- een jaarlijks terugkerend programma "de week van beveiliging & privacy".

Screening
Elke arbeidsplaats binnen Defensie wordt op basis van een risicoanalyse vastgesteld als niet-vertrouwensfunctie of als vertrouwensfunctie (niveau C, B of A). Vertrouwensfuncties zijn functies die de mogelijkheid bieden de nationale veiligheid te schaden. Medewerkers moeten in geval van plaatsing op een niet-vertrouwensfunctie, beschikken over een geldige Verklaring Omtrent Gedrag (VGG) of indien geplaatst op een vertrouwensfunctie, beschikken over een geldige

Verklaring van Geen Bezwaar (VGB). Bijna alle functies bij Defensie zijn vertrouwensfuncties. Voor beide verklaringen ondergaat betrokkene een veiligheidsonderzoek. Een veiligheidsonderzoek voor een vertrouwensfunctie is diepgaander dan een onderzoek voor een niet-vertrouwensfunctie.

2.6.4 *Norm: technische maatregelen*

Beveiliging van informatiesystemen
Voor elk informatiesysteem binnen Defensie geldt dat een aantal procedures verplicht moet worden doorlopen voordat een informatiesysteem in gebruik mag worden genomen. De goedkeuring ofwel de accreditatie voor een informatiesysteem is gebaseerd op het bestaan van een accreditatiedossier en de acceptatie van eventuele restrisico's. Het accreditatiedossier bevat tenminste een risicoanalyse als ook ingevulde "*Statement of Compliance*" voor de gebruikersorganisatie, IT-leverancier en de eigenaar. Eventuele restrisico's moeten door de daartoe verantwoordelijke lijn- en beveiligingsfunctionarissen zijn geaccepteerd voordat een accreditatie kan worden verleend. Het accreditatieproces is een complex proces waar de beoordeling op privacy aspecten standaard onderdeel van is. Als gebruik gemaakt wordt van geaccrediteerde informatiesystemen is ruim voldaan aan artikel 32 Avg voor wat betreft technische maatregelen. Daar waar informatiesystemen niet formeel het accreditatieproces of goedkeuringsproces doorlopen, blijft het DBB van toepassing en dient aan de in het DBB gestelde normen te worden voldaan.

2.7 Verantwoording

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verplichtingen van de Avg – en in het bijzonder de beginselen van de Avg – worden nageleefd bij het gebruik van het LIMC.

Dit volgt uit de in artikel 5, tweede lid, Avg opgenomen 'verantwoordingsplicht'. In deze paragraaf volgt een bespreking van de belangrijkste formele verplichtingen uit de Avg die uitvoering geven aan deze verantwoordingsplicht.

2.7.1 *Verwerkingenregister*

Een van de manieren om (deels) uitvoering te geven aan voorgaande eisen betreft het bijhouden van een verwerkingsregister (artikel 30 Avg). Voor zover de minister van Defensie verwerkingsverantwoordelijke is voor de verwerkingen binnen het LIMC, wordt dit ook verplicht op grond van artikel 2.1 en artikel 2.2 van de Regeling Avg Defensie. De artikelen 2.1 en 2.2. van deze Regeling schrijven bovendien voor op welke wijze registratie dient plaats te hebben.

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verplichtingen van de Avg – en in het bijzonder de beginselen van de Avg – worden nageleefd bij het gebruik van het LIMC.

2.7.2 *DPIA*

Een andere manier om (deels) uitvoering te geven aan voorgaande eisen betreft de uitvoering van een Gegevensbeschermingeffectbeoordeling (een zogenaamde DPIA, zie artikel 35 Avg en, voor zover de minister van Defensie verwerkingsverantwoordelijke is, artikel 3 Regeling Avg Defensie). Aan de hand hiervan, beoordeelt de verwerkingsverantwoordelijke verwerkingen, in het bijzonder verwerkingen waarbij nieuwe technologieën worden gebruikt, die gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Tevens wordt een

DPIA geïnitieerd bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien (artikel 3, lid 1 onder b Regeling Avg Defensie). Deze DPIA dient conform het model DPIA Rijksdienst te worden uitgevoerd (artikel 3, lid 2 Regeling Avg Defensie).

Bij verwerkingen en het ontwikkelen van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien dient een DPIA te worden uitgevoerd.

2.7.3 *Verwerkersovereenkomst*

Voor de toepassing van de Avg is van belang wie of wat wordt aangemerkt als verwerkingsverantwoordelijke(n), en op wie als zodanig de regels van de Avg van toepassing zijn. De verwerkingsverantwoordelijke bepaalt het doel en de middelen van de verwerking van persoonsgegevens en heeft daardoor verantwoordelijkheid voor de rechtmatigheid van de verwerking.

De verantwoordelijkheid voor de naleving van de voorgaande eisen en de overige verplichtingen uit de Avg kan eveneens liggen bij gezamenlijke verwerkingsverantwoordelijken. In dat geval dienen de verantwoordelijken gezamenlijk afspraken te maken over de naleving daarvan (artikel 26 Avg).

Daarnaast dient vastgesteld te worden of de verwerkingsverantwoordelijke voor het LIMC gebruik maakt van een verwerker. In dat geval dient de verwerkingsverantwoordelijke – door middel van (onder meer) een verwerkersovereenkomst – te borgen dat de verwerker de vereisten van de Avg strikt naleeft.

2.8 Bijzondere en strafrechtelijke persoonsgegevens

De bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens zijn persoonsgegevens die naar hun aard gevoelig zijn en waarvoor de Avg aanvullende regels stelt.[35]

De bijzondere categorieën van persoonsgegevens zijn limitatief opgesomd in artikel 9, eerste lid, Avg. Daaronder vallen bijvoorbeeld gegevens over iemands politieke opvattingen, ras, gezondheid, religie of gegevens met betrekking tot iemands seksueel gedrag.[36] Een dergelijke bijzondere categorie kan direct door het persoonsgegeven worden onthuld, maar ook indirect. In dat verband is het wel nodig, zoals de Nederlandse wetgever opmerkt bij de toelichting op de UAvg[37], dat er een rechtstreeks verband is. Gegevens die slechts een indicatie geven dat het om een bijzondere categorie zou kunnen gaan, vallen buiten de reikwijdte van artikel 9 Avg.[38]

Met name relevant in het kader van de beoordeling van de activiteiten binnen het LIMC is de bijzondere categorie gezondheid, levensovertuiging en politieke gezindheid. Het begrip gezondheidsgegevens wordt ruim uitgelegd en kan worden afgeleid uit verschillende bronnen.[39] Zo kan volgens de *European Data Protection Board* (EDPB) informatie wegens het gebruik ervan in een specifieke context, waaronder bijvoorbeeld een recente reis of verblijf in een door COVID-19 getroffen regio die bij het stellen van een diagnose is verwerkt door een zorgverlener, of informatie uit een op zelfcontrole gebaseerde vragenlijst, waarbij betrokkenen vragen over hun gezondheid beantwoorden, reeds kwalificeren als gegevens over gezondheid.[40]

De begrippen levensovertuiging en politieke gezindheid, dienen, zoals de wetgever opmerkt bij de toelichting bij de voorganger van artikel 9 Avg (artikel 16 Wbp),[41] overeenkomstig artikel 1 Grondwet en de Algemene wet gelijke behandeling uitgelegd te worden. Deze begrippen hebben in het Nederlandse recht inmiddels een gevestigde traditie. Het begrip politieke gezindheid duidt op een gemeenschappelijke opvatting omtrent de bestuurlijke en sociale inrichting van de samenleving en het begrip levensovertuiging op een gemeenschappelijke fundamentele opvatting over de samenleving en het menselijk bestaan.[42]

---

[35] Zie artikel 9 Avg; artikel 10 Avg (jo. artikel 1 UAvg); artikel 22 Avg.
[36] Vgl. artikel 4, aanhef en onder 13, Avg jo. artikel 9, eerste lid, Avg.
[37] Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 33 e.v.
[38] Zie ook 'Bijlage 1 Zienswijze Facebook Inc. en Facebook Ierland van 16 september 2015 met reactie Autoriteit Persoonsgegevens', 21 februari 2017, z2014-00929.
[39] Zie bijvoorbeeld HvJ EU van 6 november 2003, ECLI:EU:C:2003:596, C-101/01 (*Lindqvist*), par. 50.
[40] Zie EDPB, 'Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak', 21 april 2020 (raadpleegbaar via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_nl.pdf), p. 5.
[41] Zie *Kamerstukken II* 1998/97, 25 892, nr. 3.
[42] Zie College voor de Rechten van de Mens, 23 februari 2005, nr. 2005-28, rov. 5.4-5.7: "5.5 Volgens vaste jurisprudentie van de Commissie is bij godsdienst sprake van een overtuiging omtrent het leven waarbij een opperwezen centraal staat, terwijl bij een levensovertuiging dit opperwezen ontbreekt, maar er eveneens een dergelijke existentiële gemeenschappelijke overtuiging bestaat (zie CGB 4 februari 1997, oordeel 1997-15). 5.6 Volgens vaste jurisprudentie verstaat de Commissie onder levensovertuiging een min of meer coherent stelsel van ideeën, waarbij het gaat om fundamentele opvattingen over het menselijk bestaan (zie onder meer CGB 4 februari 1997, oordeel 1997-15 en CGB 5 februari 2002, oordeel 2002-04). 5.7 Ook acht de Commissie het noodzakelijk dat deze opvatting niet slechts individueel beleefd wordt, maar dat sprake is van een gemeenschappelijke opvatting (CGB 4 februari 1997, oordeel 1997-15)." (onderstreping toegevoegd). Zie voorts College voor de Rechten van de Mens, 8 maart 2011, nr. 2011-31, rov. 3.10: "Het

De verwerking van de bovengenoemde strafrechtelijke gegevens en bijzondere persoonsgegevens is verboden, tenzij hiervoor een algemene of specifieke doorbrekingsgrond bestaat in de (U) Avg of een bijzondere wet.[43]

Hieruit volgt dat bijzondere en strafrechtelijke persoonsgegevens door het LIMC slechts mogen worden verwerkt indien daarvoor een doorbrekingsgrond voorhanden is. Daarbij dient te worden opgemerkt dat een dergelijke doorbrekingsgrond de verwerkingsverantwoordelijke niet ontslaat van de plicht om een grondslag te hebben, als bedoeld in artikel 6 van de Avg.

2.8.1 *Doorbrekingsgrond: kennelijk openbaar gemaakt door betrokkene*

Een relevante doorbrekingsgrond voor de verwerking van bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens (en persoonsgegevens van strafrechtelijke aard) bij het gebruik door het LIMC, is dat de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt (zie artikel 9, tweede lid, onder e, Avg en artikel 32, onder c, UAvg).

De wetgever wijst - bij de toelichting op de soortgelijke bepaling in de Wbp[44] - op dat voor de vraag of een dergelijk persoonsgegeven kennelijk openbaar is gemaakt, de intentie van betrokkene van belang kan zijn.

Deze intentie kan worden afgeleid uit het handelen of het gedrag van de betrokkene zelf, waaronder de wijze waarop de betrokkene de informatie openbaar heeft gemaakt.

Zo is geen sprake van uitdrukkelijke openbaarmaking als een betrokkene persoonsgegevens openbaar maakt via een afgeschermd (social media) profiel. Zie de toelichting in Kamerstukken II 1997/98, 25 892, nr. 3, p. 123: [45]

"Er geldt een ontheffing voor de verwerking van gevoelige gegevens indien de gegevens door de betrokkene openbaar zijn gemaakt. Evenals bij onderdeel a ligt de rechtvaardigingsgrond voor de ontheffing besloten in het handelen of het gedrag van de betrokkene zélf. Anders dan bij onderdeel a is er echter geen sprake van op de gegevensverwerking gerichte toestemming, maar van een spontane gedraging van de betrokkene en waar niet door enig andere persoon met het oog op een eventuele gegevensverwerking om is gevraagd. Dat de gegevens openbaar zijn, moet derhalve volgen uit gedrag van de betrokkene waaruit de intentie om openbaar te maken uitdrukkelijk blijkt. Het laatste blijkt onder meer uit het feit – de Registratiekamer heeft hier terecht op gewezen – dat de richtlijn bepaalt dat de gegevens «duidelijk» door de betrokkene openbaar moeten zijn gemaakt. Dit is bijvoorbeeld duidelijk het geval in de situatie waarin een persoon die verkiesbaar is voor de volksvertegenwoordiging, zich met bepaalde politieke opvattingen in de publiciteit profileert. Het betreft hier een gegeven omtrent politieke gezindheid dat

---

begrip politieke overtuiging duidt op een gemeenschappelijke opvatting omtrent de bestuurlijke en sociale inrichting van de samenleving. Deze opvatting dient te kunnen worden afgeleid uit een bepaald handelen of nalaten van een persoon (zie: CGB 4 februari 1997, 1997-15, overweging 4.5; CGB 9 juli 2002, 2002-84, overweging 5.5; CGB 18 januari 2005, 2005-3, overweging 5.10 en CGB 21 april 2006, 2006-76, overweging 3.5)." (onderstreping toegevoegd)

[43] De algemene doorbrekingsgronden staan beschreven voor bijzondere persoonsgegevens in artikel 9, tweede lid, Avg en in artikelen 22 tot en met 30 UAvg. Voor strafrechtelijke persoonsgegevens staan deze in artikel 31 tot en met 33 UAvg.

[44] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 123.

[45] Zie ook *Kamerstukken II* 1997/98, 25 892, nr. 6, p. 42.

in beginsel door anderen mag worden verwerkt. Dat er sprake moet zijn van een intentie bij de betrokkene, blijkt ook uit de formulering van de bepaling: de gegevens moeten door de betrokkene openbaar zijn gemaakt.

Anders ligt daarom de situatie waarin een bepaald gegeven openbaar is, maar de uitdrukkelijke wens tot openbaarmaking niet door de betrokkene is geuit. Dit doet zich bijvoorbeeld voor bij personen met een handicap. Dit gezondheidsgegeven is in veel gevallen voor een ieder zichtbaar, maar niet uit vrije wil aan de kant van de betrokkene. Dit gegeven mag derhalve niet op grond onderdeel b worden verwerkt, tenzij de betrokkene zich als zodanig – bijvoorbeeld als belangenbehartiger voor gehandicapten – in de openbaarheid profileert."

De Autoriteit Persoonsgegevens verwijst naar deze passage in het Onderzoeksrapport van de Autoriteit Persoonsgegevens inzake de verwerkingen door Facebook en overweegt in dat kader:[46,47]

"Artikel 23, eerste lid, onder b, van de Wbp bepaalt dat het verbod om bijzondere persoonsgegevens te verwerken niet van toepassing is voor zover de gegevens door de betrokkene duidelijk openbaar zijn gemaakt. Er moet een uitdrukkelijke intentie van de betrokkene zijn om zelf de gegevens openbaar te maken. Deze uitzondering is niet van toepassing op gegevens die zijn verstrekt naar aanleiding van een verzoek van een verantwoordelijke."

Artikel 23, eerste lid, onder b, van de Wbp bepaalt dat het verbod om bijzondere persoonsgegevens te verwerken niet van toepassing is voor zover de gegevens door "de betrokkene" duidelijk openbaar zijn gemaakt.

---

[46] Autoriteit Persoonsgegevens, 'Onderzoek naar het verwerken van persoonsgegevens van betrokkenen in Nederland door het Facebook-concern', z2014-00929, 21 februari 2017, p. 102.

[47] Net als in de volgende richtsnoeren van de voorganger van de Autoriteit Persoonsgegevens: College bescherming persoonsgegevens, 'Publicatie van gegevens op het internet', december 2007 (raadpleegbaar via:https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rs/rs_20071211_persoonsgegevens_op_internet_definitief.pdf), p. 14 en 15.

2.8.2 *Doorbrekingsgrond: noodzakelijk voor wetenschappelijk onderzoek/statistische doeleinden*

Een andere relevante doorbrekingsgrond is dat de verwerking noodzakelijk is met het oog op wetenschappelijk onderzoek of statistische doeleinden overeenkomstig artikel 89, eerste lid, Avg[48] op grond van Unierecht of lidstatelijk recht (artikel 9, tweede lid, onder j, Avg en artikel 32, onder f, UAvg)[49,50]. Om daarvan gebruik te kunnen maken dient er wel sprake te zijn van onderzoek dat kwalificeert als wetenschap of statistisch onderzoek. De (voorganger en de) EDPB wijst erop dat het "wetenschappelijk onderzoek" niet verder kan worden opgerekt dan de gebruikelijke betekenis en vat het begrip in deze context op "als een onderzoeksproject dat opgezet wordt in overeenstemming met de relevante methodologische en ethische normen van de sector, en conform goede praktijken."[51]

---

[48] Zie artikel 89, eerste lid, Avg: 'De verwerking met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden is onderworpen aan passende waarborgen in overeenstemming met deze verordening voor de rechten en vrijheden van de betrokkene. Die waarborgen zorgen ervoor dat er technische en organisatorische maatregelen zijn getroffen om de inachtneming van het beginsel van minimale gegevensverwerking te garanderen. Deze maatregelen kunnen pseudonimisering omvatten, mits aldus die doeleinden in kwestie kunnen worden verwezenlijkt. Wanneer die doeleinden kunnen worden verwezenlijkt door verdere verwerking die de identificatie van betrokkenen niet of niet langer toelaat, moeten zij aldus worden verwezenlijkt.'

[49] jo. artikel 24 UAvg.

[50] Volgens overweging 159 van de considerans van de Avg "moet de verwerking van persoonsgegevens met het oog op wetenschappelijk onderzoek ruim worden opgevat en bijvoorbeeld technologische ontwikkeling en demonstratie, fundamenteel onderzoek, toegepast onderzoek en uit particuliere middelen gefinancierd onderzoek omvatten. Bovendien dient de doelstelling van de Unie uit hoofde van artikel 179, lid 1, VWEU, te weten de totstandbrenging van een Europese onderzoeksruimte, in acht te worden genomen. Wetenschappelijke onderzoeksdoeleinden omvatten ook studies op het gebied van de volksgezondheid die in het algemeen belang worden gedaan."

[51] Zie ook EDPB, 'Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak', 21 april 2020 (raadpleegbaar via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_nl.pdf) en Zie de Artikel 29-Werkgroep, 'Richtsnoeren inzake toestemming overeenkomstig Verordening 2016/679', WP259 versie 01, 17/NL, blz. 27 (bekrachtigd door de EDPB) (raadpleegbaar via: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051).

3 Bevindingen

Dit hoofdstuk beschrijft de relevante feiten en omstandigheden op basis van het onderzoek. Allereerst wordt de context van de verwerking geschetst gevolgd door de opdracht aan het LIMC. Daarna wordt de organisatie en het proces van het LIMC uiteengezet. Het hoofdstuk wordt afgesloten met een beschrijving van de organisatorische en technische maatregelen die het LIMC heeft getroffen.

3.1 Context

De eerste Nederlander is op 27 februari 2020 positief getest op de ziekte COVID-19. Het aantal besmettingen neemt daarna snel toe. Op 11 maart 2020 noemt de World Health Organization (WHO) de corona-uitbraak officieel een pandemie.[52] Vanaf 12 maart zijn in heel Nederland maatregelen getroffen die tot doel hebben het coronavirus onder controle te krijgen en de zorg niet te overbelasten.[53] Defensie heeft zich voorbereid om de eigen organisatie tegen de effecten van het virus te beschermen en de Nederlandse autoriteiten te ondersteunen in de crisis.

Een context van onzekerheid[54]

"De uitbraak van COVID-19 vormde een grote bedreiging voor de Nederlandse samenleving. Afschrikwekkende beelden uit Italië, de premier die voor het eerst sinds de oliecrisis het volk toespreekt en ons land voorbereidt op een situatie met beperkte bewegingsvrijheid en ziekenhuizen die vollopen met COVID-patiënten.

De beginperiode van de landelijke aanpak van deze crisis kenmerkte zich door het op gang komen van de civiele command en control structuren en de inrichting van de afstemmingsfora binnen de overheid.

Te verwachten impact op de landmacht

Al snel werd duidelijk dat de impact op de krijgsmacht en dus ook de landmacht substantieel zou zijn. In de landen om ons heen zagen we ook de inzet van krijgsmachten ter ondersteuning van civiele autoriteiten. Een dergelijk beroep van civiele autoriteiten op de krijgsmacht was in Nederland te verwachten. Tevens was de inschatting dat de COVID-19 pandemie impact zou hebben op de continuering van de bedrijfsprocessen van de landmacht alsmede de gereedstelling en inzet van landmacht-personeel in de uitzendgebieden.

Behoefte aan overzicht

In een dergelijke – chaotische – situatie is het militair gebruik om zo snel mogelijk een overzicht van de toestand te genereren en indien mogelijk een inschatting voor planningsdoeleinden. Deze stap in de militaire commandovoering heet de evaluatie van de toestand. Dit om (1) de negatieve effecten van de COVID-19 pandemie voor de inzetbaarheid van landmacht-personeel voor reguliere bedrijfsvoering zoveel mogelijk te beperken; om (2) de negatieve effecten van de COVID-19 pandemie voor gereedstelling en instandhouding van CLAS-eenheden voor internationale operaties zoveel mogelijk te beperken; en om (3) voorzorgsmaatregelen te treffen zodat we klaar zouden staan voor het geval de Nederlandse samenleving een beroep

---

[52] Tedros, (2020, 11 maart), https://www.who.int/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020.
[53] Kamerstukken II 2019/20, 25295, nr. 508.
[54] Ministerie van Defensie (2021, 21 januari). 20210121 Commandanten appreciatie LIMC. Utrecht: Staf Clas / Kabinet

op ons zou doen om op korte termijn militaire bijstand en steun te verlenen ter ondersteuning van civiele autoriteiten betrokken bij de crisisbestrijding.

De behoefte aan een zo volledig mogelijk omgevingsbeeld gold ook voor de civiele instanties. Zo bleek al vanaf het begin van de crisis toen het ministerie van BZK aan alle betrokken overheidsorganisaties vroeg om informatie te delen.

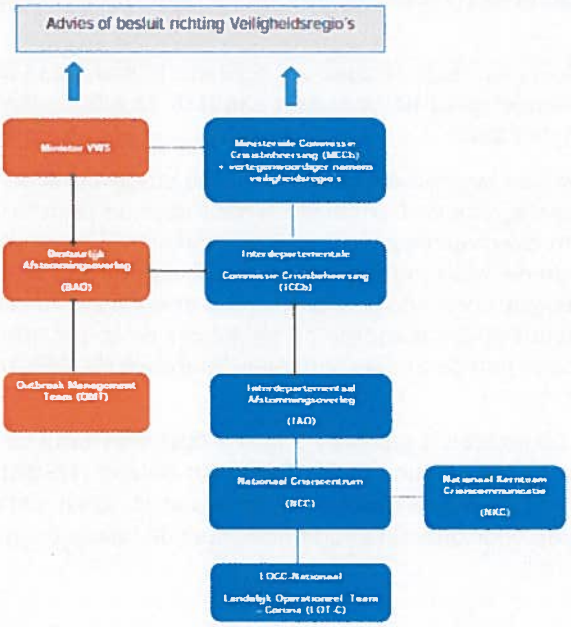
Oogmerk minister-president

De overheid is onder aanvoering van de minister-president de COVID-19 pandemie gaan bestrijden. Al direct was duidelijk dat met 50% van de informatie wel 100% van de besluiten genomen moest worden. De minister-president gaf dan ook zonder omhaal van woorden aan (bij herhaling): "alleen samen krijgen we corona er onder"."

3.1.1 *Crisisstructuur operationeel/tactisch Nederland*

De gezamenlijke coördinatie en aanpak op operationeel-tactisch niveau is vormgegeven via de werkwijze Landelijk Operationeel Coördinatiecentrum-Nationaal (LOCC-N) / Landelijk Operationeel Team-Corona (LOT-C). Het gaat hier om een multidisciplinair samenwerkingsverband tussen alle hulpverleningsdiensten, Defensie, bevolkingszorg, veiligheidsregio's en ministeries. [55]

Grafische weergave van de crisisstructuur COVID-19:



Figuur 1: Crisisstructuur COVID-19[56]

De nationale crisisstructuur is ingericht tot en met 1 juli 2020. In de zomer is de Ministeriële Commissie COVID-19 (MCC-19) ingericht om integraal over het beleid

[55] Kamerstukken II 2019/20, 30821/25295, nr. 107.
[56] Kamerstukken II 2019/20, 30821/25295, nr. 107.

ten aanzien van de bestrijding en de gevolgen van COVID-19 te besluiten. Dat zijn aanvullingen op de beschreven crisisstructuur[57].

Bij de civiele centra en teams zijn militairen als liaisons werkzaam. De liaison onderhoudt contacten met Defensie, waaronder het Tactisch Operationeel Centrum (TOC) van het Commando Landstrijdkrachten (CLAS). Vanuit het TOC worden militaire (crisis)operaties op Nederlands grondgebied gecoördineerd en aangestuurd.

3.1.2 *Besluitvorming bij nationale inzet[58]*

'(...)De inzet van defensiemiddelen voor nationale taken, militaire bijstand of steun geschiedt altijd onder gezag en op verzoek van civiele autoriteiten. Defensie is daarbij complementair aan de ingezette civiele middelen.

Een aanvraag voor bijstand of steunverlening komt binnen bij het Defensie Operatiecentrum van de DOPS. In alle gevallen wordt overlegd met de Directeur Juridische Zaken (DJZ). Het verlenen van toestemming voor militaire bijstand is de bevoegdheid van de minister van Veiligheid en Justitie. De minister van Veiligheid en Justitie bepaalt met de minister van Defensie op welke wijze bijstand wordt verleend. De bevoegdheden van de minister van Defensie zijn gemandateerd aan de secretaris-generaal.

Deze bevoegdheid is, afhankelijk van het soort verzoek, (door)gemandateerd aan de CDS of de DJZ. Indien sprake is van een verzoek op grond van de Politiewet om militaire bijstand aan de politie door de KMar geldt het mandaat van de secretaris-generaal.

Indien sprake is van een verzoek om militaire bijstand aan de politie door 'groen' defensiepersoneel geldt het mandaat van DJZ. In alle andere gevallen ligt het mandaat bij de CDS.

Het verlenen van toestemming voor militaire steunverlening is een interne defensieaangelegenheid. De minister wordt door de secretaris-generaal geïnformeerd over verzoeken tot steunverlening of bijstand en op de hoogte gehouden van de voortgang en beëindiging van de inzet. De besluitvormingsprocedure kan snel worden doorlopen. Zo wordt verzekerd dat Defensie adequaat kan reageren op bijstands- en steunverleningsverzoeken. Functionarissen van de Sectie Nationale Operaties (DOPS) en van de DJZ zijn 24/7 beschikbaar. (...)'

Tijdens het onderzoek is gebleken dat het opstellen van een aanvraag op basis van een Militaire Steunverlening in het Openbaar Belang (MSOB) of militaire bijstand in de praktijk lastig werd gevonden omdat de capaciteiten van de krijgsmacht en de mogelijkheden voor ondersteuning onvoldoende bekend zijn bij het civiel gezag.

3.1.3 *Informatiegestuurd optreden/Information Manoeuvre*

Defensie ziet informatiegestuurd optreden als een belangrijke eigenschap van Defensie in de toekomst. In de Defensievisie 2035[59] is dit als volgt verwoord:

---

[57] Kamerstukken II 2020/21, Handelingen, Aanhangsel 430.
[58] Introductiebundel Defensie oktober 2017, https://www.rijksoverheid.nl/documenten/publicaties/2017/10/27/introductiebundel-defensie
[59] Kamerstukken II, 2020/21, 34919, nr. 71.

'We specialiseren ons in het opbouwen en behouden van een gezaghebbende informatiepositie.

Dit is de basis voor een sterke focus op informatiegestuurd optreden (IGO), dat minder gericht is op afbakeningen in tijd en locatie.

Daarmee kunnen we relevante en betrouwbare informatie snel vergaren, verwerken, analyseren en daar uiteindelijk snel en beslissend mee handelen en mee vechten, van strategisch niveau tot het niveau van de individuele militair in het veld.

We vergroten en versnellen, met de juiste informatie, onze handelingsperspectieven voor inzet. Alleen op die manier kunnen we mogelijke tegenstanders bijhouden en met meer maatwerk reageren. De informatieomgeving is van groeiend belang en is een terrein waarop zogeheten hybride dreigingen goed gedijen. Denk daarbij bijvoorbeeld aan maatschappij ontwrichtende cyberaanvallen en desinformatiecampagnes. We gaan ervan uit dat we multidomein en geïntegreerd moeten optreden, veelal in een hybride context. Met onze partners buiten Defensie gaan we meer conceptuele aandacht besteden aan de rol en taak van Defensie in dit grijze gebied van 'strategische competitie' tussen vrede en oorlog.'

Vastgesteld is dat op dit moment nog geen DPIA is opgesteld voor IGO.

Wat is Informatiegestuurd Optreden?[60]

De Koninklijke Landmacht definieert Informatiegestuurd Optreden (IGO) als: 'alle relevante data en informatie kunnen verwerven, verwerken en verspreiden teneinde *insight, foresight* en *understanding* te creëren en tijdig op elk niveau en in elke situatie militaire besluitvorming en militair optreden in drie dimensies (cognitief, virtueel en fysiek) te kunnen realiseren'. Het gaat hierbij nadrukkelijk om zowel de dagelijkse bedrijfsvoering als de operationele omgeving.

Toegespitst op militaire inzet in de informatieomgeving noemt de Koninklijke Landmacht dit '*Information Manoeuvre*'. Net zoals *ground-* en *air manoeuvre*, heeft *Information Manoeuvre* tot doel een voordeel of gunstige positie ten opzichte van opponenten te bereiken. Dit gebeurt door de cognitieve, virtuele en fysieke dimensie te exploiteren, integraal te begrijpen, daarop besluitvorming te baseren en vervolgens met activiteiten (offensieve en defensieve) effecten te realiseren. Het doel van *Information Manoeuvre* is het beïnvloeden van wil, gedrag en/of perceptie van opponenten en andere relevante actoren met alle vormen van slagkracht.

3.2 Opdracht LIMC

Op 19 maart 2020, heeft Commandant Landstrijdkrachten een Operatieorder[61] (OPORD 2020-710 (COVID-19)) uitgegeven. In een aantal (aanvullende) orders

[60] Visie informatiegestuurd optreden voor de Landmacht, Manoeuvreren in de informatieomgeving, november 2020.

[61] Operation order (OPORD) A directive, usually formal, issued by a commander to subordinate commanders for the purpose of effecting the coordinated execution of an operation, Joint Doctrine Publicatie 5 Commandovoering.

(*Fragmentary Orders* (FRAGO[62])) wordt de opdracht in bevelvorm nader uitgewerkt. Zoals in de FRAGO NO. 003 bij OPORD 2020-710 (COVID-19)[63] van de Directeur Training en Operaties CLAS waarin hij de Commandant van het Operationeel Ondersteuningscommando Land (C-OOCL) opdraagt:

> *(1) Richt in en lever in DS aan TOC een Land Information Manoeuvre Centre (LIMC) om binnen de vigerende regelgeving en ICCW KMAR bij te dragen aan de SASU van CLAS teneinde een bijdrage te kunnen leveren aan civiele overheden.*

C-OOCL geeft in zijn OPERATIEBEVEL NO. 2020-025 (COVID-19) en de FRAGO 001 de volgende opdracht en oogmerk mee:

> *(...)*
> *(3) Land Information Manoeuvre Center (LIMC)*
> *(a) OOCL heeft de opdracht om een LIMC in te richten en DS aan het TOC te leveren, IOC op 231400AMRT20, om binnen de vigerende regelgeving en ICCW KMAR bij te dragen aan de SA/SU van CLAS teneinde een bijdrage te kunnen leveren aan civiele overheden.*
> *(b) Oogmerk C-OOCL mbt LIMC: Bouw een Land Information Manoeuvre Centre, waarin OOCL capaciteiten worden samengebracht, teneinde digitale en analoge producten ten behoeve van civiele en militaire besluitvorming te leveren.*
> *(c) C-LIMC wordt een directe ondercommandant van C-OOCL*
> *(d) LIMC is een experimentele eenheid welke op- c.q. afgeschaald kan gaan worden n.a.v. behoefte en vraag. Reguliere eenheden OOCL dienen er rekening mee te houden dat zij naar behoefte en in opdracht van C-OOCL personeel, materieel en/of diensten ter beschikking stellen aan het LIMC.*
>
> *Evaluatie van de commandant: De COVID-19 crisis heeft een grote impact op de maatschappij, beslissers in crisisorganisaties binnen en buiten Defensie hebben behoefte aan analyse capaciteit om op diverse functiegebieden overzicht te krijgen over de Impact van de crisis op de maatschappij. Dit vraagt om een grondige multidisciplinaire aanpak, zodat wij inzicht krijgen in de gevolgen van de crisis, vervolgens begrijpen wat dit betekent voor de maatschappij en mogelijk aanbevelingen kunnen doen die de besluitvorming van de beslissers ondersteunt.*
>
> *Oogmerk: Door geïntegreerde, gecoördineerde en doelmatige (economy of effort) Inzet van OOCL capaciteiten, worden producten gemaakt in DS aan het hoger niveau. Beschouw alle beschikbare en relevante informatie, uit open en semi-gesloten bronnen, over de COVID-19 crisis, teneinde SA-SU te genereren voor CLAS en civiele overheden IRT COVID-19 crisis. Hierdoor worden militaire en civiele besluitvormingsprocessen gevoed met inzicht en waar mogelijk handelingsperspectief.*

In het bevel van de C-OOCL staat IOC voor *Initial Operational Capability* 231400AMRT20 is de datum tijdgroep, met ICCW wordt *in close coorporation with* (in samenwerking met KMar) bedoeld en *SA/SU* is de afkorting voor *situational awareness/situational understanding* ("weten wat er speelt in de omgeving"/begrijpen wat er gebeurt"). Met andere woorden: op 23 maart 2020 om 14.00 uur dient het LIMC ingericht te zijn. De datum dat het LIMC gereed is *(Full*

[62] Fragmentary order (FRAGO) An abbreviated form of an operation order, issued as required, that eliminates the need for restating information contained in a basic operation order. It may be issued in sections, Joint Doctrine Publicatie 5 Commandovoering.
[63] FRAGO 003 bij OPERATIEORDER 2020-710 (COVID-19), 19 maart 2020.

Operational Capablility) volgt later.[64] In bijlage III is een organogram van Defensie, de Koninklijke Landmacht en het OOCL opgenomen.

In FRAGO 004 bij operatiebevel 2020-039 van C-OOCL is de taak van het LIMC als volgt verwoord:

> *(...)*
>
> *Algemeen*
>
> *Het Land Information Manoeuvre Centre (LIMC) genereert in een experimentele vorm Situational Awareness (SA) en Situational Understanding (SU) voor het CLAS en civiele overheden over de COVID-19 crisis. Hierdoor worden militaire en civiele besluitvormingsprocessen gevoed met inzicht en waar mogelijk handelingsperspectief. Door het inrichten van het LIMC draagt het OOCL op een slimme manier bij aan het continueren van de essentiële processen binnen de Nederlandse samenleving en Defensie in tijden van crisis.*
>
> *Dit past in de dóórontwikkeling naar een Informatie Gestuurde Krijgsmacht, om met behulp van nieuwe technologieën en beter gebruik van informatie, het militaire optreden te verbeteren. Hierdoor kunnen ook nieuwe bedreigingen het hoofd geboden worden. Met het LIMC kan de Koninklijke Landmacht ervaring opdoen met het samenbrengen van information manoeuvre capaciteiten die insight, foresight en doorlopend handelingsperspectief bieden in drie dimensies (cognitief, virtueel, fysiek).*
>
> *(...)*

3.3 Organisatie LIMC

Het LIMC was en is geen organieke eenheid binnen het CLAS. Medewerkers zijn dan ook niet geplaatst bij het LIMC maar voor korte of langere tijd vanuit bestaande eenheden of organisaties gevraagd of aangewezen om activiteiten te verrichten. De meeste medewerkers zijn militairen (beroeps en reservisten), ook zijn enkele burgermedewerkers en niet-werknemers (zoals stagiaires en medewerkers van partnerorganisaties) bij het LIMC ingezet. De kern van het LIMC is gevormd met medewerkers van het JISTARC[65] op de Luitenant-kolonel Tonnetkazerne in 't Harde. De lijst met (voormalig) medewerkers van het LIMC is verstrekt door de *acting* chef-staf van het LIMC en bevat de namen van 151 personen. De groepsgrootte varieert in omvang door de tijd heen. Sommige personen hebben kort gewerkt voor het LIMC en anderen enkele maanden, soms op roulatiebasis. De meeste medewerkers zijn tijdelijk deels vrijgemaakt van hun organieke werkzaamheden en hadden daarnaast nog hun organieke functie met bijbehorende taken en opdrachten.

In de enquête is uitgevraagd hoelang medewerkers werkzaamheden tussen maart en november 2020 hebben verricht voor het LIMC. De resultaten van de 106 respondenten zijn als volgt:

---

[64] OPERATIEBEVEL NO. 2020-025 (COVID-19) en FRAGO 001 BIJ OPERATIEBEVEL NR 2020-025 (COVID-19), 20 maart 2020

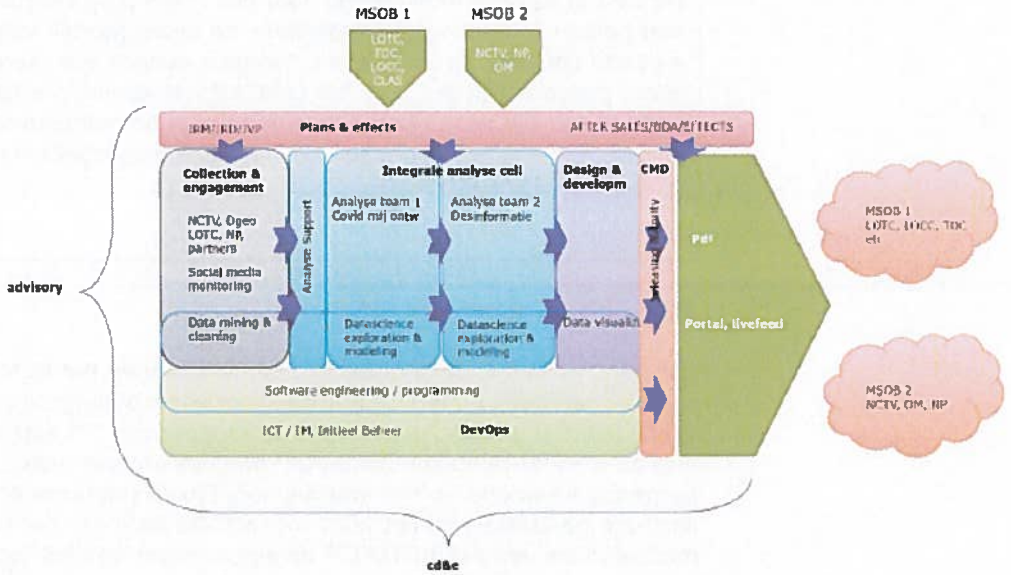
[65] Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando is een inlichtingeneenheid. Het commando verzamelt, analyseert en verspreidt inlichtingen in een inzetgebied. Daarmee helpt de eenheid met name commandanten ter plekke bij het plannen van operaties en andere besluitneming.

Hoelang heeft u in totaal werkzaamheden verricht voor het LIMC?	Telling	Column N %
minder dan 1 week	3	2,9%
een week	1	1,0%
tussen 1 week en 1 maand	16	15,4%
tussen 1 maand en 3 maanden	42	40,4%
langer dan 3 maanden	42	40,4%

Tabel 1: Duur werkperiode personen werkzaamheden voor het LIMC

3.4 Proces LIMC

Het proces van het LIMC is als volgt toegelicht tijdens een toezichtbezoek:



Figuur 2: LIMC proces[66]

Uit nader toegezonden informatie is het LIMC proces als volgt verduidelijkt:

Het LIMC proces start met het initiëren, sturen en begeleiden van de binnengekomen vragen en vervolgens het stellen van prioriteiten op basis van de twee hoofdthema's van het LIMC: maatschappelijke ontwikkelingen/gevolgen COVID-19 en desinformatie in relatie tot COVID-19.

In het informatieverzamelplan (IVP)[67] wordt vanuit de geformuleerde hoofdthema's de informatiebehoefte en de (potentiële) bronhouders inzichtelijk gemaakt.

Vervolgens wordt de binnengekomen informatie verwerkt tot integrale producten. De analyse was hiervoor georganiseerd in twee teams. Team 1: maatschappelijke ontwikkelingen/gevolgen COVID-19. Team 2: desinformatie in relatie tot COVID-19.

Dit leidt tot de wekelijkse rapportages ontwikkeld door *Design & Dissemination*. Waarna de *Releasing authority* zorgt voor de interne review- en kwaliteitscheck op

[66] CD-E voortgangverslag LIMC 200608.
[67] informatieverzamelplan LIMC 21 juli 2020 (laatste update 5 oktober 2020).

o.a. de gestelde kaders. Ook werd er door een medewerker naar de processen gekeken om vast te kunnen stellen wat er op termijn nodig was, in het kader van *learning by doing* (*advisory*).

In de enquête is uitgevraagd waar medewerkers werkzaamheden hebben uitgevoerd. De resultaten zijn als volgt:

Waar binnen het LIMC heeft u werkzaamheden uitgevoerd? (meerdere keuzes mogelijk)		Telling
Integrale analyse cell (team 1 Covid ontwikkeling)	Ja	34
Integrale analyse cell (team 2 Desinformatie)	Ja	23
Collection & Engagement	Ja	18
Design & Development	Ja	10
Data OPS	Ja	9
CMD	Ja	4
Plans & Effects	Ja	8
CD&E	Ja	7
Wil ik niet zeggen	Ja	2
Anders		86

Tabel 2: Capaciteit per cell

3.4.1 *Methodiek analyseteams*

In de teams is gebruik gemaakt van een methodiek. Deze methodiek bestaat uit vier stappen:

1. *Data mining & cleaning*
2. *Datascience exploration & modeling*
3. Datavisualisatie
4. Verstrekken van informatie

De vier stappen worden hieronder toegelicht.

Stap 1: *Data mining & cleaning*
Allereerst wordt de opdracht geanalyseerd en zo nodig de onderzoeksvraag geherformuleerd. Hierbij is gebruik gemaakt van zogenaamde "narratieven". Een narratief is een gestructureerd verhaal over fenomenen of maatschappelijke ontwikkeling, bij het LIMC COVID-19 gerelateerd.

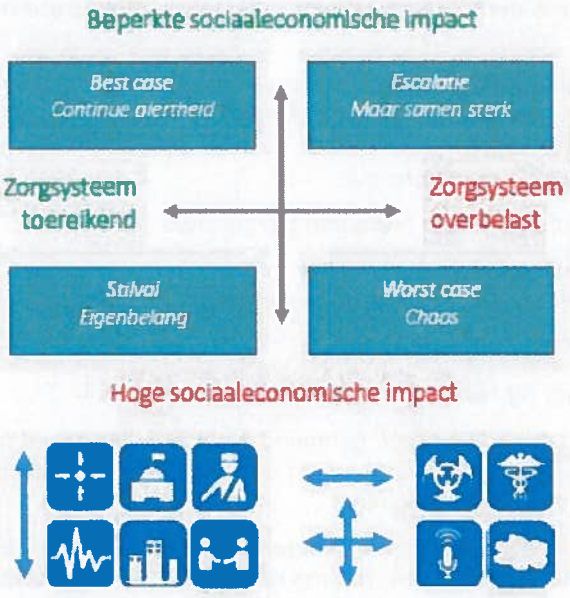
Een apart team ook wel *cell* genoemd hield zich bezig met analyseren en het visueel weergeven van de gegevens. Vanaf eind mei 2020 is het team gesplitst in twee teams van circa 5-6 personen.

Het eerste "team zorg" heeft zich gericht op de zorg zoals beddencapaciteit en de verwachte IC opnamen. Hierbij maakt het LIMC gebruik van tien door het LOT-C onderkende factoren van invloed. Visueel ziet dit er als volgt uit:

Factor		Factor	
	1. Virus		6. Vitale infrastructuur
	2. Zorg		7. Economie
	3. Continuïteit van bestuur		8. Destabilisering (niet) statelijke actoren
	4. Openbare orde & Veiligheid		9. Communicatie & media
	5. Burgerschap		10. Meteo, evenementen & incidenten

Figuur 3 Factoren van invloed[68]

Het LOT-C heeft tien (10) primaire factoren van invloed gedefinieerd. Op de assen van het maatschappelijk kompas staan twee (2) factoren van invloed die de grootste impact hebben. Op de horizontale as staat de impact van COVID-19 op de zorg. Op de verticale as staat de sociaaleconomische impact weergegeven. Op basis van vier (4) kwadranten kunnen vervolgens scenario's worden gebouwd.



Figuur 4 Scenario's maatschappelijk kompas[69]

Vastgesteld is dat het team zorg gebruik heeft gemaakt van kwantitatieve gegevens.

[68] 20200924-DV-LIMC-WEEKLY_COVID-19_week_39
[69] 20200924-DV-LIMC-WEEKLY_COVID-19_week_39

Het tweede team heeft zich gericht op desinformatie gerelateerd aan COVID-19. Het tweede team is ook aangeduid als "team desinformatie". Dit team heeft narratieven of thema's onderzocht met als hoofdvraag: in hoeverre beïnvloedt des- en misinformatie in relatie tot COVID-19 de Nederlandse samenleving? Voorbeelden[70] van de narratieven in dit team zijn:

Naam narratief	Omschrijving
5G	Volgens dit narratief zouden mensen door 5G straling vatbaarder zijn voor COVID-19 doordat het immuunsysteem aangetast zou worden, of zelfs dat 5G-zenders het virus verspreiden.
Anti-vaccinatie	Het anti-vaccinatie narratief beweert dat het coronavirus in laboratoria is gecreëerd en doelmatig losgelaten zou zijn, onder meer om microchips in te brengen om de wereldbevolking te controleren. Tevens zou dit virus ontworpen zijn om veel winst te maken met de verkoop van verplichte vaccins.
Rusland versus EU	Het narratief gaat over het actief verspreiden van desinformatie door aan Rusland gelieerde partijen met als doel om maatschappelijke verdeeldheid te creëren binnen de EU. In het narratief wordt Nederland zelf niet direct als doelwit gezien, maar kunnen Nederlandse belangen in het buitenland wel geschaad worden door desinformatie. Ook kan de eenheid binnen de EU op den duur in gevaar komen.
Virus	Het narratief gaat over de invloed van pseudowetenschappelijk onderzoek op de publieke opinie over de getroffen maatregelen tegen COVID-19. Onderzoeken van traditionele onderzoeksinstituten worden betwist door actiegroepen die zich baseren op (eigen) pseudowetenschappelijk onderzoek naar het virus. Het narratief omvat alle mis/desinformatie die gebruikt wordt als verzet tegen het huidige COVID-19 beleid.

Tabel 3: Narratieven

Bij de narratieven is gewerkt met een mate van waarschijnlijkheid in relatie tot de gegeven duiding, conclusies of assessments. Hierbij is gebruik gemaakt van onderstaande tabel waarin de mate van waarschijnlijkheid is toegelicht.

[70] Weekly update desinformatie, 21 juli 2020.

Terminologie	*Confidence* level
Hoogstwaarschijnlijk	80-90%
Waarschijnlijk	60-80%
Mogelijk	40-60%
Onwaarschijnlijk	20-40%
Hoogst onwaarschijnlijk	0-20%

Tabel 4: Waarschijnlijkheid

Indeling medialandschap
Het desinformatieteam monitorde het Nederlandse medialandschap. Hierbij hanteerde het een indeling van traditionele, niet-traditionele en alternatieve media. In interviews en tijdens het toezichtbezoek is in een presentatie toegelicht dat deze indeling afkomstig is uit onderzoek van het Rathenau Instituut.[71]

- 'Traditionele nieuwsmedia: bedrijven en organisaties die vanuit journalistiek oogpunt nieuws en/of actualiteiten aanbieden, gebruikmakend van de journalistieke principes van hoor- en wederhoor. Deze nieuwsmedia zijn vaak wel gelieerd aan een bepaalde politieke kleur, maar rapporteren wel genuanceerd.
- Niet traditioneel: nieuwsmedia die niet algemeen nieuws en/of actualiteiten aanbieden maar bijvoorbeeld specifiek over een bepaald onderwerp of vanuit een bepaalde blik op de wereld. Deze nieuwsmedia kunnen minder genuanceerd zijn dan traditionele nieuwsmedia, of volledig ongenuanceerd.
- Alternatieve media: bronnen die een alternatieve zienswijze bieden dan de (niet) traditionele media.'

Desinformatie
Gehanteerd is het begrip desinformatie zoals omschreven door het *Europese High Level Expert Group on Fake News and Online disinformation*: 'onware, inaccurate of misleidende informatie die intentioneel wordt gecreëerd en verspreid omwille van economisch profijt of om een persoon, sociale groep, organisatie of land te schaden'.

De medewerkers van de analyseteams zijn analisten die voor het merendeel afkomstig zijn van 106 Inlichtingencompagnie (106INLCIE), een eenheid van het JISTARC. Deze analisten zijn bekend met *Open Source Intelligence*, vaak afgekort als OSINT, in het verzamelen van data en informatie uit open en publiek beschikbare bronnen. Deze gegevens worden verzameld, geanalyseerd en op een begrijpelijke gerapporteerd of gepubliceerd.

Het onderzoek heeft zich geconcentreerd op het tweede team omdat daar het grootste risico op verwerking van persoonsgegevens was. Dit is bevestigd uit steekproeven van gebruikte databronnen, interviews en opgeleverde producten.

Stap 2: *Datascience exploration & modeling*
In de tweede stap worden gegevens verzameld om de onderzoeksvraag te beantwoorden.

Hierbij heeft het LIMC onderstaande databronnen gebruikt. Het volledige overzicht is departementaal vertrouwelijk gerubriceerd, onderstaand een selectie van het overzicht.

[71] Presentatie OSINT Proces/werkwijze.

Nr.	Organisatie bron	Data/Info	Type	Frequentie
1	KMAR	CTER Today	PDF	Onregelmatig
2	NCTV	Wekelijks maatschappelijk beeld (Dashboard)COVID-19	PDF	Wekelijks
3	MIN VWS	Dashboard	SITE	Dagelijks
4	CZSK	DUB COMNLCARIB N2	PPT	Dagelijks
5	EU	Daily Covid Headlines EU	MAIL	Dagelijks
6	Defensie/DCO	Dagelijks Nieuwsupdate	MAIL	Dagelijks
7	CLAS	Dagelijks CUB TOC	PDF	Dagelijks
8	EU	IPCR enquête + ISAA rapportage	PDF	Onregelmatig
9	Instituut Fysieke Veiligheid	Landelijk operationele COVID_19 monitor	PDF / JPEG	Wekelijks
10	Nationale Politie	Corona Crime Change Monitor	PDF	Tweewekelijks
11	CLAS	Assessment indicatoren economie	WORD	Wekelijks
12	CLAS	Dagelijks Zip	ZIP	Dagelijks
13	KMAR	Landelijk operationeel beeld COVID-19	PDF	Wekelijks
14	KMAR	Overzicht grenspassages (AMIGO BORAS)	PDF	Wekelijks
15	CLAS	Wekelijkse voorspelling Corona patiënten op IC + Appreciatie	WORD / PNG / PPT	Wekelijks
16	EU	CoronaVirusOutbreak Europe EEAS	PDF	Dagelijks
17	RIVM	COVID-19_WebSite_rapport (Epidemiologische situatie)	PDF	Wekelijks
18	Instituut Fysieke Veiligheid	Ale relevante rapporten in de verschillende domeinen	PDF	Dagelijks
21	CLAS	Duiding vanuit standpunt viroloog	WORD	Wekelijks
22	Defensie/DCO	Rapporten ivm burgerlijke gehoorzaamheid en naleving	PDF	Onregelmatig
23	CLAS	Grafieke berichtgeving (Factoren en narratieven)	EXCEL	Wekelijks

Nr.	Organisatie bron	Data/Info	Type	Frequentie
24	CLAS	OSINT Rapport	WORD	Wekelijks
25	KWR	Data rioolwater	EXCEL	Gestopt
26	Defensie/DGO	Information about Infection Desease Update	PDF	Tweewekelijks
27	Landelijk Coördinatiecentrum Patiënten Spreiding	Dagrapportage IC bezetting	PDF + datastroom	Dagelijks
28	CLAS	Wekelijkse buitenlandmelding (oefeningen)	EXCEL	Wekelijks
29	CLAS	Sociaal maatschappelijke update	Word	Wekelijks
30	CBS	Dashboard verschillende thema's	DASHBOARD	Permanent
31	NIVEL	Verschillende publicaties ivm zorg en Covid-19	PDF	Wanneer beschikbaar
32	CLAS	SJP STCLAS 2020 (Overzicht alle oefeningen)	EXCEL	Permanent
33	RIVM	.CSV bestand met datametingen rioolwater	EXCEL	Wekelijks

Tabel 5: Databronnen[72]

Sommige bronnen bevatten alleen kwantitatieve gegevens en bevatten geen persoonsgegevens, andere bronnen zijn kwalitatief van aard. Voorbeelden van kwantitatieve rapportages zonder persoonsgegevens zijn het overzicht grenspassages en de Landelijk coördinatiecentrum patiëntenspreiding (LCPS) dagrapportage (IC-bezetting). Een voorbeeld van een kwalitatieve rapportage zonder persoonsgegevens is de *Daily Covid Headlines EU*. Tijdens het onderzoek is aan de hand van steekproeven vastgesteld dat in enkele rapportages namen voorkomen van publieke figuren of in bronvermeldingen. Een voorbeeld hiervan is de Contra Terrorisme Extremisme en Radicalisering *Today* (*CTER Today)*. Dit rapport aangeleverd door de KMar is DEPARTEMENTAAL VERTROUWELIJK gerubriceerd, bevat geen politiegegevens maar bevatte bijvoorbeeld de namen van de aanslagplegers in Parijs op 13 en 14 november 2015. Daarnaast zochten medewerkers van het LIMC aan de hand van stap 1 gericht, handmatig in open bronnen (*open source)* op internet.

Bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens

Vastgesteld is dat het LIMC in beperkte mate namen en functies heeft verwerkt. Sommige namen en functies zijn van bekende politici. Dit zijn bijzondere persoonsgegevens omdat hieruit een politieke opvatting blijkt.

[72] Informatieverzamelplan LIMC, 21 juli 2020, (laatste update 5 oktober 2020).

Tijdens interviews is aangegeven dat andere bijzondere persoonsgegevens niet zijn verwerkt. Ook de enquête uitkomsten bevestigen dit.

Wel is vastgesteld dat het LIMC in het laatste kwartaal 2020 heeft verkend of strafrechtelijke gegevens (zoals boetes en handhaving coronamaatregelen) beschikbaar zouden zijn.

OSINT, (sociale) media- en sentimentanalyse
Het overzicht databronnen (tabel 5) bevat ook een wekelijkse OSINT (*Open Source Intelligence*) rapportage. OSINT is het verzamelen van data en informatie uit open en publiek beschikbare bronnen. Een OSINT rapportage bevat een overzicht en analyse van bepaalde informatie uit voor een ieder toegankelijke bronnen. Deze gegevens worden verzameld, geanalyseerd en op een begrijpelijke manier gerapporteerd of gepubliceerd. Voor het analyseren van dergelijke informatie, is gebruik gemaakt van *tools* waaronder Coosto.

In mei en juni zijn de technische mogelijkheden van de tools waaronder Meltwater en Coosto en de juridische- en Avg aspecten met betrekking tot sentimentanalyses verkend. In de zomer van 2020 is door één medewerker op een privé laptop gestart met de sentimentanalyse, woordenwolk en een activiteitendiagram. Hierbij is gebruik gemaakt van de *tools* Coosto en Meltwater met door Defensie verstrekte licenties. Door de medewerker is aangegeven dat voornamelijk gebruik gemaakt is van Coosto. Meltwater is na een korte verkenning niet verder gebruikt.

Coosto

Coosto is een bedrijf dat gespecialiseerd is in het *scrapen* van sociale mediaberichten van het internet. Uit een verkennend onderzoek van het CBS [73] blijkt in 2019 dat Coosto in de praktijk vooral berichten van Twitter (tweets en retweets) en in mindere mate Facebook, LinkedIn, Instagram, Pinterest, blogs en nieuws betrekt.

Citaten privacyverklaring Coosto[74]:

'(...)Coosto verzamelt data om openbare bronnen voor gebruikers doorzoekbaar te maken.
Gebruikers bepalen zelf hoe en waarvoor ze de Coosto-software gebruiken. Ze zijn daarbij wel gebonden aan Coosto's gebruikersvoorwaarden.
Zo kunnen zij de webcare-module gebruiken om vragen over hun product of dienst op social media te zoeken en deze te beantwoorden. Met social media management & analyse kunnen bedrijven en organisaties bijvoorbeeld over een langere termijn meten wat de effectiviteit is van hun marketingcampagnes of trends in de markt detecteren om hierop in te kunnen spelen en hun merk te versterken. Coosto wordt ook gebruikt voor statistische toepassingen door onder andere onderwijs- en wetenschapsinstellingen, non-profitorganisaties, gemeenten en studenten. Coosto's publishingdienst helpt bedrijven bij het managen van hun marketingcampagnes. Ze kunnen plannen wanneer informatie naar buiten wordt gebracht en de reacties daarop meten.

[73] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiWnJKZn93uAhWI-6QKHd_jATsQFjACegQIAxAC&url=https%3A%2F%2Fwww.cbs.nl%2F-%2Fmedia%2F_pdf%2F2019%2F16%2Fgebruik-van-sociale-media.pdf&usg=AOvVaw2t-YUGtlQZLsaR68MExkFI.
[74] https://www.coosto.com/nl/privacyverklaring, 9 maart 2020.

Door openbare informatie makkelijk doorzoekbaar te maken, helpt Coosto haar klanten om betere beslissingen te nemen over hun bedrijfsstrategieën. Juridisch gezegd beroept Coosto zich op het gerechtvaardigd belang van Coosto en haar gebruikers om deze beslissingen mogelijk te maken.'

Verwerkingsverantwoordelijke/verwerker:

'(...)Voor verwerkingen van persoonsgegevens die Coosto op eigen initiatief verricht, zoals het verwerken van eigen klantdata, geldt Coosto als de 'verantwoordelijke' in de zin van de privacyregelgeving. Dat betekent kort gezegd dat Coosto (formeel: Coosto B.V.) als bedrijf verantwoordelijk is voor de naleving van deze regelgeving. Daarnaast kan Coosto voor bepaalde verwerkingen van persoonsgegevens 'verwerker' zijn in de zin van de privacyregelgeving. Bij die diensten gelden de klanten van Coosto als verwerkingsverantwoordelijken. (...)'

De overeenkomst van Defensie met Coosto heeft een ingangsdatum van 1 september 2020 en is gesloten onder de rijksinkoopvoorwaarden voor diensten (ARVODI-2018). Een Avg verwerkersovereenkomst is niet aangetroffen.

Daarnaast is aangegeven dat geen zoektermen zijn gebruikt met persoonsgegevens. Vastgesteld is dat in mei en juni 2020 een presentatie en overleg heeft plaatsgevonden met juristen en Avg coördinatoren over de werkwijze.

Naar aanleiding van dit overleg zijn onderstaande specifieke instellingen (filters) in Coosto ingesteld. Hierdoor zijn uitsluitend "media" en bedrijfspagina's op Facebook gebruikt bij de verwerking.

Vastgesteld is dat hiervoor een specifiek "leeg" Facebookaccount is aangemaakt omdat anders de bedrijfspagina's op Facebook niet konden worden betrokken in de sentimentanalyse.

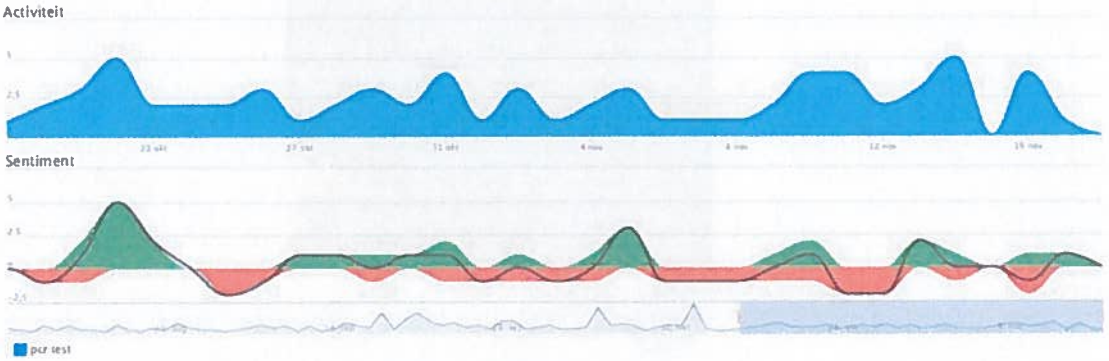
Onderstaand het Facebookaccount en de getoonde instellingen in Coosto:

Figuur 5: Facebookaccount

Figuur 6: Getoonde instellingen Coosto

Het door de medewerker opgeleverde product bestaat uit drie elementen:

- Een sentimentanalyse. Dit betreft een kwantitatief overzicht met media-artikelen (alleen open bronnen) over een bepaald onderwerp. In de analyse wordt er onderscheid gemaakt tussen negatief, positief en neutraal sentiment. Een voorbeeld uit de praktijk betreft het onderwerp PCR Test. Hierbij is gebruik gemaakt van de volgende zoekcriteria: PCR Test : (pcrtest | pcr-test | pcr) ((kort geding) | betrouwb*).



Figuur 7: Voorbeeld sentimentanalyse [75]

Figuur 8: Voorbeeld sentimentanalyse[76]

- Een woordenwolk (*wordcloud*). Hoe groter het woord is afgebeeld hoe vaker het voorkomt. De medewerker heeft aangegeven dat gebruik gemaakt is van woordenwolken:
    - met *tags* (sleutelwoorden op nieuwssites);
    - meest gebruikte woorden in zoekresultaten;
    - met *hashtags* (# meest gebruikte sleutelwoorden op social media door een # aangegeven).

  Indien in de woordenwolk namen voorkwamen zijn deze verwijderd. Hierna is een afbeelding in Powerpoint gemaakt van de woordenwolk, deze afbeelding is opgenomen in de rapportage. Voorbeeld:

[75] Media & Webcarerapport nummer 12, november 2020.
[76] Media & Webcarerapport nummer 12, november 2020.

Figuur 9: Voorbeeld woordenwolk [77]

- Een activiteitendiagram waarmee visueel de media-aandacht voor een onderwerp kan worden weergegeven.

De conceptrapportage is daarna aangeboden aan de contactpersoon bij JISTARC/109OSINT die voor verdere verspreiding in de analysecell ook nog een check uitvoerde op afwezigheid van persoonsgegevens.

In de praktijk bleek de sentimentanalyse voor het LIMC niet bruikbaar. De informatie bleek achteraf te beperkt om betrouwbare tellingen weer te geven.

Stap 3: Datavisualisatie
Het LIMC heeft de narratieven visueel en tekstueel toegelicht in de producten zoals de *Weekly's*.

Prominente publieke functies/Publieke figuren
In de producten zijn namen en functies van personen die een prominente publieke functie[78] vervullen zoals ministers en staatshoofden niet gelakt. Dit geldt ook voor namen en functies van publieke figuren. Het betreft personen die politieke of maatschappelijke verantwoordelijkheid dragen, (andere) bekende Nederlanders, en anderen die zich in het publieke debat mengden.

Namen en functies in bronvermeldingen
De bronvermelding verwijst naar de oorspronkelijke, openbaar toegankelijke documenten of teksten. Behalve namen en functies van personen gaat dit ook om informatie betreffende de sociale en maatschappelijke context. Bijvoorbeeld een naam van een natuurlijke persoon wordt volgens een krantenartikel in verband gebracht met bepaalde feiten, beweringen of meningen over het COVID-19 virus.

Na de start van het LIMC is voor de gehanteerde werkwijze expliciet aandacht besteed aan het voorkomen van verwerking van persoonsgegevens.

Daarnaast is bij twijfel, in een latere fase, met regelmaat contact opgenomen met juristen en Avg deskundigen. Op basis van verkregen advies hebben medewerkers van het LIMC ten onrechte aangenomen dat verwerken van persoonsgegevens van

---

[77] Media & Webcarerapport nummer 12, november 2020.
[78] Uitwerking van artikel 2 van het Uitvoeringsbesluit Wwft 2018, witwassen. Het is een lijst van prominente publieke functies in de definitie van politiek prominente personen (Politically Exposed Persons, PEP) in Nederland.

publieke figuren en bronvermeldingen geen persoonsgegevens zouden zijn en dat de verwerking van deze gegevens onder de Avg was toegestaan.

Vastgesteld is dat een DPIA niet is opgesteld voor de verwerking van persoonsgegevens door het LIMC en evenmin een melding in het Avg verwerkingenregister Defensie is gedaan.

Vastgesteld is dat namen en functies van personen die een prominente publieke functie vervullen niet weggelaten of verwijderd werden dan wel laat in het verwerkingsproces deels zijn gepseudonimiseerd (bijvoorbeeld vervangen door xx).

In de enquête is ook gevraagd of medewerkers in aanraking zijn gekomen met persoonsgegevens en of hierbij sprake was van publieke figuren en/of bronvermeldingen. Onderstaand de resultaten:

Hoe vaak bent u voor uw werkzaamheden voor het LIMC in aanraking gekomen met persoonsgegevens?		Telling	Column N %
	nooit	56	56,0%
	soms	19	19,0%
	noch soms, noch vaak	8	8,0%
	vaak	9	9,0%
	heel vaak	7	7,0%
	wil ik niet zeggen	1	1,0%

Tabel 6: In aanraking met persoonsgegevens

Op welke categorie personen hebben deze persoonsgegevens betrekking? (meerdere antwoorden mogelijk)		Telling
politici/bestuurders	Ja	31
journalisten	Ja	17
wetenschappers	Ja	23
influencers	Ja	17
belangengroepen (woordvoerders)	Ja	22
zorgmedewerkers	Ja	8
defensiemedewerkers	Ja	16
politie/brandweer	Ja	9
Anders		105

Tabel 7: Categorie personen

In welke mate hebben deze persoonsgegevens betrekking?		Telling	Column N %
(Onder een "publiek figuur" wordt verstaan: alle personen die politieke of maatschappelijke verantwoordelijkheid dragen, bekende Nederlanders, en anderen die zich in het publieke debat mengen)	nooit	12	27,9%
	soms	5	11,6%
	noch soms, noch vaak	3	7,0%
	vaak	5	11,6%
	heel vaak	17	39,5%
	weet ik niet/wil ik niet zeggen	1	2,3%

Tabel 8: Publiek figuur

Hoe vaak kwam u in aanraking met artikelen waarin een naam vermeld staat?		Telling	Column N %
	nooit	6	14,0%
	soms	9	20,9%
	noch soms, noch vaak	6	14,0%
	vaak	15	34,9%
	heel vaak	6	14,0%
	weet ik niet/wil ik niet zeggen	1	2,3%

Tabel 9: Hoe vaak in aanraking met persoonsgegevens

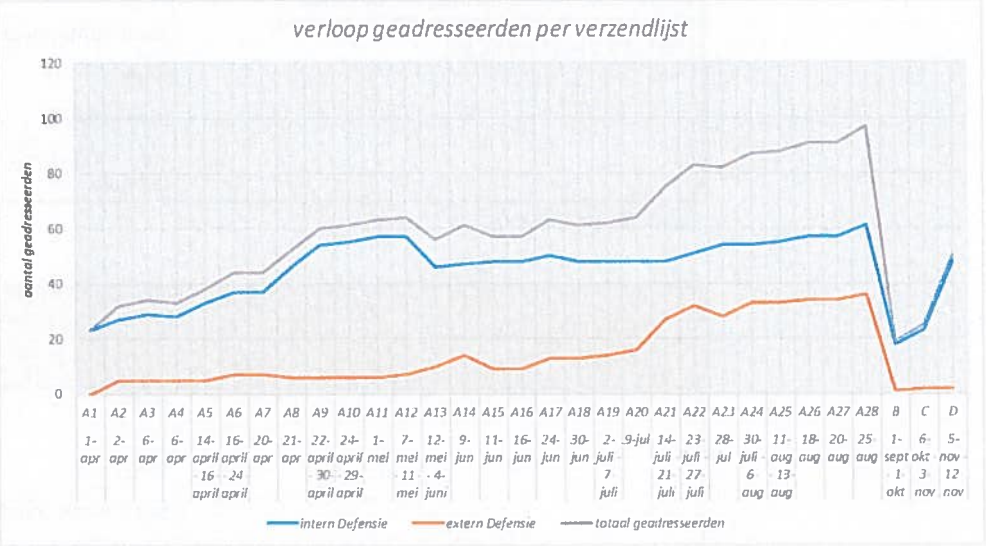
Stap 4: Verstrekken van informatie

Drie perioden

Onderscheid wordt gemaakt in drie perioden:

- In de periode maart-mei 2020, zijn dagelijks zorggerelateerde rapportages verstrekt.
- In de periode mei-augustus 2020, is het analyseteam gesplist. Team 1: maatschappelijke ontwikkelingen/gevolgen COVID-19. Team 2: desinformatie in relatie tot COVID-19. Wekelijks zijn rapportages verspreid aan een ruime doelgroep. Zo heeft het LIMC informatieproducten geleverd aan onder andere: Nationale Politie, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Nationaal Coördinator Terreurbestrijding en Veiligheid (NCTV), Landelijk Operationeel Team Corona (LOT-C), Landelijk Operationeel Coördinatiecentrum (LOCC), Actiecentrum Koninklijke Landmacht (ACKL) Territoriaal Operatiecentrum (TOC) en Directeur Operaties (DOPS). De verzendlijst bestond maximaal uit 94 geadresseerden, waarvan ongeveer de helft e-mailadressen binnen het ministerie van Defensie en de helft overheidsinstanties buiten Defensie waren.
- In de periode september–november 2020 is de verspreiding van LIMC rapportages beperkt tot afnemers intern Defensie. Hiertoe is op 27 augustus

besloten. Afnemers ontvingen het volgende bericht van het LIMC: *"Afgelopen week is uit interne heroverwegingen gebleken dat het niet meer opportuun is periodiek rapportages te verzenden. Mocht er desondanks een behoefte zijn om producten te ontvangen vanuit het LIMC, kunt u hiervoor een steunverzoek richten aan het Ministerie van Defensie via de reguliere procedure."*



Figuur 10 verloop geadresseerden

- Naast verzending van de rapportages per e-mail werd informatie uit de rapportage tevens gepresenteerd tijdens de dagelijkse *Commanders Update Brief* (CUB) via de *Environment Cell* van het TOC. De rapportages geven omgevingsbeeld en bevatten voorspellingen over hoe de toestand in Nederland zich als gevolg van de corona-crisis zou kunnen ontwikkelen.

Persoonsgegevens in rapportages

Het onderzoeksteam heeft van het LIMC initieel een bestand ontvangen met daarin alle verzonden e-mails van de functionele mailbox uit de onderzoeksperiode. Dit bestand bevat 79 e-mails met meerdere bijlagen, vijf bijlagen zijn later nagezonden. In totaal heeft het onderzoeksteam hieruit 80 rapportages geanalyseerd op de verwerking van (bijzondere) persoonsgegevens. In bijlage IV zijn de analyseresultaten gedetailleerd opgenomen.

Vastgesteld is dat in 34 rapportages persoonsgegevens zijn verwerkt. Het betreft "bijvangst". Sommige persoonsgegevens, zoals die van publieke figuren en bronvermeldingen zijn opgenomen omdat medewerkers van het LIMC na verkregen advies dachten dat dit volgens de Avg was toegestaan. Vastgesteld is dat hierover overleg heeft plaatsgevonden en dat het LIMC op dit punt onjuist advies heeft ontvangen.

De aangetroffen persoonsgegevens hebben betrekking op 50 unieke natuurlijke personen. Hiervan zijn namen of functies verwerkt in de tekst (inhoud) van de rapportages of in de bronvermeldingen.

Deze informatie is deels direct herleidbaar tot een natuurlijk persoon op basis van een persoonsnaam en deels indirect herleidbaar bijvoorbeeld op basis van functieaanduiding.

3.5 Organisatorische en technische maatregelen

3.5.1 *Organisatorische maatregelen*

Het LIMC bestaat uit meerdere groepen die verschillende processtappen binnen het primaire proces van het LIMC uitvoerden om via deelproducten te komen tot eindproducten.

Geheimhoudingsverklaring
Alle medewerkers van Defensie hebben een verklaring omtrent de bekendheid met de geheimhoudingsplicht ondertekend bij aanstelling of andere relatie met Defensie. Dit is verplicht en eenmalig. De medewerkers van het LIMC hebben een separate geheimhoudingsverklaring ondertekend. Dit is een aanvullende organisatorische maatregel.

Beveiligingsbriefing
Medewerkers van Defensie zijn op verschillende manieren op de hoogte gebracht van beveiliging & privacy. Daar waar organisatieonderdelen hiertoe specifieke activiteiten ontplooien zoals een jaarlijkse briefing en rouleer procedures geldt dat deze aanvullend zijn.

Bij het LIMC is gaandeweg een briefing ontwikkeld waarin aandacht wordt besteed aan beveiliging en de Avg. Deze briefing is, naast de standaard briefings binnen Defensie, gegeven aan het merendeel van de medewerkers die voor of bij het LIMC hebben gewerkt.

Screening
Alle militairen en veel burgermedewerkers bij Defensie vervullen een vertrouwensfunctie. Zij hebben voor hun aanstelling een veiligheidsonderzoek gehad en beschikken over een Verklaring van Geen Bezwaar (VGB). Alle medewerkers die betrokken zijn bij het LIMC beschikken over minimaal een Verklaring Omtrent Gedrag (VoG) maar in de meeste gevallen over een Verklaring van Geen Bezwaar op minimaal het niveau staatsgeheim CONFIDENTIEEL. Dit niveau overstijgt het niveau van gemerkte informatie. Het onderzoeksteam heeft een gerichte steekproef gehouden naar het beschikken over een juiste VoG of VGB. In alle gecontroleerde gevallen was dit juist; daarmee blijkt deze organisatorische maatregel effectief.

De normen van het DBB met betrekking tot organisatorische maatregelen, zijn nageleefd.

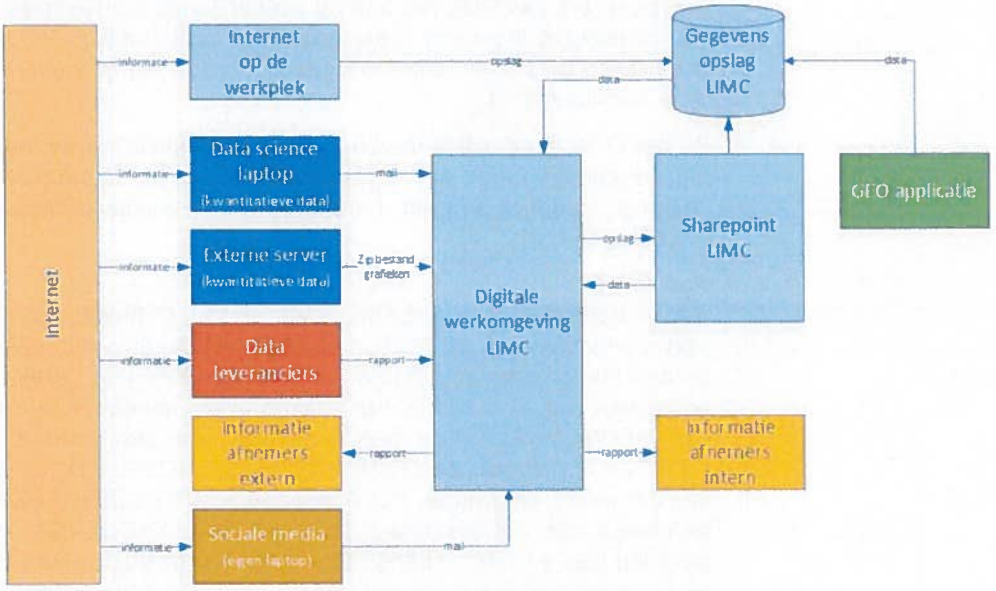
3.5.2 *Technische maatregelen*

Om te bepalen of wordt voldaan aan de technische norm maakt het onderzoeksteam gebruik van het *Input, Throughput* en *Output* model. Daarbij staat bij *Input* het verzamelen van informatie centraal, bij *Throughput* het analyseren en verwerken en bij *Output* het eindproduct.
Tijdens het onderzoek is vastgesteld dat persoonsgegevens, zij het als bijvangst, worden verwerkt in alle onderdelen van dit model. Per processtap is onderzocht of gebruik wordt gemaakt van geaccrediteerde informatiesystemen. De resultaten zijn in onderstaande tabel weergegeven:

Processtap	Verwerking Persoonsgegevens	Gebruik geaccrediteerde systemen	Gebruik niet geaccrediteerde systemen
Input	X	X	X
Throughput	X	X	-
Output	X	X	-

Tabel 10: Input, Throughput en Output model

Uit de interviews is gebleken dat het LIMC voornamelijk door Defensie verstrekte en geaccrediteerde informatiesystemen heeft gebruikt zoals het reguliere bedrijfsvoering netwerk MULAN en de operationele variant TITAAN. Globaal zien de informatiestromen binnen het LIMC er als volgt uit:



Figuur 11: Informatiestromen LIMC

Daarnaast is vastgesteld dat gebruik gemaakt is van een eigen Netwerk en *Network-attached storage* (NAS), een niet geaccrediteerd systeem. De NAS is wel voorzien van beveiligingsmaatregelen zoals toegangsbeheersing, anti-virus software, Virtual Machine, VPN en deze bevindt zich binnen de invloedsfeer van de voor de beveiliging verantwoordelijke functionaris.

Tijdens het onderzoek is vastgesteld dat gebruik is gemaakt van één privé laptop voor processtap *Input*. De privé laptop betrof een niet door Defensie verstrekt IT-middel waarop wel beveiligingsmaatregelen waren getroffen maar die feitelijk buiten het controlebereik van de defensieorganisatie stond en getroffen beveiligingsmaatregelen niet vooraf zijn geverifieerd aan de hand van de DBB normen. Hierdoor voldeed de laptop niet aantoonbaar aan het DBB.

Tenslotte geldt naast alle technische maatregelen die zijn getroffen binnen systemen ook dat deze systemen, met uitzondering van de privé laptop, zijn gehuisvest op defensieobjecten en daarbinnen in gesloten omgevingen. Deze gesloten omgevingen zijn voorzien van toegangsbeheersing en indringer-detectiesystemen.

De normen van het DBB met betrekking tot technische maatregelen zijn nageleefd met uitzondering van het gebruik van een privé laptop hier is de norm niet aantoonbaar nageleefd.

4 Conclusies en aanbevelingen

Op basis van het toetsingskader zijn bevindingen beoordeeld. Dit heeft geleid tot onderstaande conclusies en aanbevelingen.

Conclusies

1. Vastgesteld is dat het LIMC persoonsgegevens heeft verwerkt. Dit gebeurde niet grootschalig en zonder de intentie om persoonsgegevens te verwerken. Het LIMC heeft COVID-19 gerelateerde maatschappelijke ontwikkelingen als "fenomeen" in kaart gebracht om militaire en civiele besluitvorming te voeden met inzicht en handelingsperspectief.

   Het LIMC heeft gegevens uit algemeen toegankelijke bronnen, waaronder nieuwswebsites en sociale mediaplatforms, verzameld, geanalyseerd en verwerkt in rapportages. Lang niet in alle gevallen ging het daarbij om persoonsgegevens, maar bijvoorbeeld om statistische gegevens van IC-opnames en besmettingsaantallen. Het uitvoeren van zoekopdrachten en het raadplegen van persoonsgegevens via het internet zijn wel verwerkingen en vallen dus onder het toepassingsbereik van de Avg.

   Het onderzoek heeft daarnaast aangetoond dat in de rapportages nog persoonsgegevens van (publieke) personen voorkomen. Ook het tijdens of voorafgaand aan het analyse- en productieproces verwijderen van persoonsgegevens uit de rapporten ('pseudonimiseren'), is een verwerking van persoonsgegevens en ook daarop is de Avg van toepassing. Sommige persoonsgegevens zoals die van publieke figuren en bronvermeldingen zijn in rapportages opgenomen omdat medewerkers van het LIMC na verkregen advies dachten dat dit volgens de Avg was toegestaan. Vastgesteld is dat hierover overleg heeft plaatsgevonden en dat het LIMC op dit punt onjuist advies heeft ontvangen.

2. Vastgesteld is dat het LIMC bijzondere persoonsgegevens heeft verwerkt, dit betreft persoonsgegevens over politieke opvattingen. Het gaat om namen en functies van bekende politici en bestuurders. In voorkomende gevallen zal het gaan om bijzondere persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt. De doorbrekingsgrond: kennelijke openbaarheid door de betrokkene, zou mogelijk van toepassing zijn als de wettelijke grondslag voldeed. Andere bijzondere categorieën van persoonsgegevens zijn door het onderzoeksteam niet aangetroffen. De interviews en de enquête uitkomsten bevestigen dit.

3. Het doel van de verwerking is vooraf omschreven in de operatiebevelen van de Commandant Landstrijdkrachten en de Commandant Operationeel Ondersteuningscommando Land. In het kort: militaire en civiele besluitvorming voeden met inzicht en handelingsperspectief in relatie tot COVID-19. Dit doel is gezien de context voldoende welbepaald, maar niet gerechtvaardigd omdat de wettelijke grondslag ontbreekt zoals bedoeld in artikel 6, eerste lid, Avg. De verwerking voldoet daarmee ook niet aan het rechtmatigheidsbeginsel, als bedoeld in artikel 5 Avg. Het civiel gezag heeft geen verzoek gedaan om militaire bijstand of militaire steunverlening in het openbaar belang (MSOB) en de minister van Defensie heeft geen zelfstandige taak en/of bevoegdheid waarop de nationale inzet van het LIMC kan berusten.

4. Het LIMC was en is geen organieke eenheid binnen het CLAS. Medewerkers zijn dan ook niet geplaatst bij het LIMC maar voor korte of langere tijd vanuit bestaande eenheden of organisaties gevraagd of aangewezen om activiteiten te verrichten.

   De logging, autorisatie en toegang tot systemen en gegevensbronnen is bij het LIMC ingericht conform de stringente normen van het Defensiebeveiligingsbeleid (DBB).

   Informatieproducten van het LIMC zijn zowel binnen als buiten Defensie verspreid. De verzendlijst bevat maximaal 94 geadresseerden, waarvan ongeveer de ene helft e-mailadressen binnen het ministerie van Defensie en andere helft overheidsinstanties buiten Defensie. Er was geen grondslag of taak voor de nationale inzet van het LIMC ten behoeve van civiele autoriteiten. Er was geen grondslag om producten van het LIMC die persoonsgegevens bevatten te verstrekken aan personen of instanties binnen of buiten het ministerie van Defensie.

5. Omdat persoonsgegevens werden verwerkt was een melding van deze activiteiten in het Avg verwerkingenregister Defensie noodzakelijk. Deze melding is niet gedaan.

6. De Avg-regelgeving schrijft voor dat ook bij een beleidsinitiatief, zoals het concept *Information Manoeuvre*, voorafgaand aan de verwerking een DPIA vereist is. Dit is niet gebeurd.

7. De normen van het DBB zijn nageleefd voor wat betreft organisatorische maatregelen als geheimhoudingsverklaring, beveiligingsbriefing en screening. Op het gebied van technische maatregelen is vastgesteld dat bij *throughput* en *output* gebruik is gemaakt van geaccrediteerde informatiesystemen waarmee ruimschoots is voldaan aan de norm. Voor *input* is vastgesteld dat naast geaccrediteerde informatiesystemen gebruikgemaakt van een privé laptop met beveiligingsmaatregelen die niet aantoonbaar voldoen aan de norm.

Eindconclusie

Het LIMC heeft COVID-19 gerelateerde maatschappelijke ontwikkelingen als "fenomeen" in kaart gebracht om militaire en civiele besluitvorming te voeden met inzicht en handelingsperspectief. Het LIMC had niet de intentie om (grootschalig) persoonsgegevens te verwerken, maar is hierin niet volledig geslaagd. Persoonsgegevens kwamen mee als "bijvangst".

Voor deze verwerking bestond geen wettelijke grondslag en is niet voldaan aan de verantwoordingsplicht waardoor de Avg onvoldoende is nageleefd.

Aanbevelingen

De Functionaris Gegevensbescherming beveelt de minister van Defensie aan:

1. *Stel een (beleids-) DPIA op voor Informatiegestuurd optreden*
   In de Defensievisie 2035 is Informatiegestuurd optreden (IGO) de basis van de toekomstige defensieorganisatie. Het verwerken van persoonsgegevens is hierbij onvermijdelijk. Soms valt de verwerking van persoonsgegevens onder de Wet inlichtingen- en veiligheidsdiensten 2017, de Wet politiegegevens of is een uitzondering voor inzet van de krijgsmacht aan de orde waardoor de Avg materieel niet van toepassing is. Bij andere verwerkingen van persoonsgegevens is de Avg wel van toepassing. Gezien de soort van de verwerking is een hoog privacyrisico waarschijnlijk en is daarom een (beleids-)DPIA vereist.

2. *Actualiseer de Catalogus Nationale Operaties 2018*
   Wet- en regelgeving bepaalt de mogelijkheden voor de inzet van de krijgsmacht, ook bij nationale taken. Afspraken over de beschikbare capaciteit en aanvraagprocedures voor civiel-militaire samenwerking zijn onder meer vastgelegd in de Catalogus Nationale Operaties 2018. Die biedt een overzicht van de inzetmogelijkheden van de krijgsmacht op Nederlands grondgebied door middel van steunverlening en bijstand aan de overheid. Het verdient aanbeveling om bij de volgende actualisatie van de catalogus daarin een omschrijving van de taken, verantwoordelijkheden, bevoegdheden en mogelijkheden van de krijgsmacht op het gebied van *information manoeuvre* en andere militaire analysecapaciteit op te nemen.

3. *Hanteer willen, mogen en kunnen in de juiste volgorde*
   Ontwikkelingen bij de krijgsmacht moeten binnen de kaders van wet- en regelgeving de (technische) mogelijkheden en het beoogde doel worden beschouwd. Met andere woorden, vragen in verband met willen, mogen en kunnen moeten in de juiste volgorde worden gesteld én beantwoord.
   Indien behoefte bestaat aan wijziging van regelgeving, bijvoorbeeld door ontwikkelingen in het informatiedomein, is wetgeving vereist. Voordat deze behoefte wordt overwogen is het antwoord op de "willen" vraag noodzakelijk.

4. *Versterk de poortwachtersfunctie op het gebied van gegevensverwerking*
   Verhoog bij behoeftestellers en inkopers structureel het risicobewustzijn van het verwerken van persoonsgegevens bij de verwerving van *webbased* producten en diensten ten behoeve van het informatiedomein. Maak, zoals voorgeschreven, gebruik van de model Avg verwerkersovereenkomsten.

5. *Inventariseer risicovolle verwerkingen van persoonsgegevens*
   Inventariseer in 2021 verwerkingen met persoonsgegevens bij Defensie waarbij getwijfeld wordt of de principes van de Avg in voldoende mate worden nageleefd en prioriteer deze mede aan de hand van de DPIA criteria in de Avg.

6. *Versterk en professionaliseer de Avg organisatie*
   Versterk en professionaliseer de Avg organisatie en schenk daarbij in het bijzonder aandacht aan de Avg coördinatiefunctie en aan de samenwerking met de juridische en operationele lijn. Voorzie in een risicogerichte invulling van de Avg-organisatie door bij eenheden zoals OOCL/JISTARC fysiek een Avg-coördinator onder te brengen. Geef in samenspraak met de FG invulling aan de functie van een *Chief Privacy Officer (CPO)*[79] en positioneer deze binnen de BS/DBE.

[79] Naar analogie van de motie van het lid Verhoeven c.s. over een chief privacy officer bij uitvoeringsorganisaties. Kamerstukken II 2020/21, 27529 nr. 239

Bijlage I: Aankondiging toezichtbezoek LIMC

Ministerie van Defensie

DEPARTEMENTAAL VERTROUWELIJK

Bestuursstaf
Directoraat Generaal Beleid
Directie Beleid & Evaluatie
Functionaris Gegevensbescherming

Kalvermarkt 32
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Contactpersoon

Datum
18-11-2020

Onze referentie
BS2020023515

Aantal pagina's incl. bijlage(n)
4

Bij beantwoording datum, onze referentie en onderwerp vermelden

Van: Functionaris Gegevensbescherming Defensie

Aan: Commandant Landstrijdkrachten

Afschrift: (P)SG, CDS
DGB, DGB/DBE, DJZ, DGB/CIO
C-OOCL, C-JISTARC, C-LIMC (C-DIVI)

Betreft: Aankondiging toezichtbezoek LIMC

AANKONDIGING TOEZICHTBEZOEK LIMC

De Minister van Defensie dient als verwerkingsverantwoordelijke passende technische en organisatorische maatregelen te treffen om te waarborgen en te kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de geldende privacy wet- en regelgeving wordt uitgevoerd. Dit betreft bij Defensie de Algemene verordening gegevensbescherming (Avg), de Uitvoeringswet Avg en de op basis van deze wetten geldende onderliggende besluiten en regelingen[1].

De Functionaris voor Gegevensbescherming (FG) Defensie fungeert als de wettelijke interne toezichthouder op de naleving van de geldende wet- en regelgeving ter bescherming van persoonsgegevens.

De Autoriteit Persoonsgegevens kan op grond van de Avg[2] als onafhankelijke externe toezichthouder onderzoek doen naar de naleving van de privacywetgeving en handhaven met corrigerende maatregelen, zoals een verwerkingsbeperking of verwerkingsverbod, bestuurlijke boetes of een last onder dwangsom. Contacten met de Autoriteit Persoonsgegevens (AP) geschieden door tussenkomst van de FG.

Op grond van de Avg-regeling Defensie bent u aangewezen als Avg-beheerder en belast met de zorg voor de naleving van de Avg voor verwerkingen van persoonsgegevens binnen het Operationeel Commando Landstrijdkrachten.
U dient als Avg-beheerder, belast met de zorg voor de naleving van de Avg, er voor zorg te dragen dat persoonsgegevens op een rechtmatige, behoorlijke en transparante wijze worden verwerkt.

1 Daarnaast is op de MIVD de Wet inlichtingen- en veiligheidsdiensten van toepassing en op de Koninklijke Marechaussee de Wet Politiegegevens, die in dit document buiten beschouwing blijven.
2 De bevoegdheden van de AP zijn opgenomen in artikel 58 Avg en artikel 83 Avg.

DEPARTEMENTAAL VERTROUWELIJK

DEPARTEMENTAAL VERTROUWELIJK

Bestuursstaf
Directoraat Generaal Beleid
Directie Beleid & Evaluatie
Functionaris Gegevensbescherming

Datum
18-11-2020

Onze referentie
BS2020023515

Gelet op;

- de berichtgeving over de activiteiten van het Land Information Manoeuvre Center (LIMC) in het NRC Handelsblad op 16 november 2020[3] en de reactie daarop vanuit Defensie[4], waaruit het beeld naar voren komt dat er binnen de experimenteeromgeving van het LIMC mogelijk sprake is van incidenten aangaande het verwerken van persoonsgegevens;
- het feit dat het LIMC, of de experimenteeromgeving, onderdeel zijn van het Operationeel Ondersteuningscommando Land (OOCL) van de Koninklijke Landmacht.

Overwegende;

- dat op grond van artikel 38 Avg en de regeling Avg Defensie de FG naar behoren en tijdig dient te worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens;
- dat het op grond van artikel 30 Avg en artikel 2.2. van de Regeling Avg Defensie verplicht is een register van verwerkingsactiviteiten bij te houden van de verwerkingen van persoonsgegevens die onder verantwoordelijkheid van Defensie binnen de Koninklijke Landmacht plaatsvinden;
- dat het op grond van artikel 35 Avg en artikel 3 Regeling Avg Defensie voorafgaande aan het starten van nieuwe verwerkingen die waarschijnlijk een hoog risico inhouden voor betrokkenen, verplicht is een data protection impact assessment (DPIA) uit te voeren;
- dat het op grond van artikel 35 Avg en artikel 3 Regeling Avg Defensie voorafgaande aan de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien, verplicht is om een DPIA uit te voeren;
- dat op grond van artikel 35 lid 2 Avg en artikel 3 Regeling Avg Defensie bij het uitvoeren van een DPIA het advies van de FG dient te worden ingewonnen;
- dat er op grond van artikel 32 Avg en artikel 6 Regeling Avg Defensie passende technische en organisatorische beveiligingsmaatregelen moeten zijn getroffen ter voorkoming van verlies en onrechtmatige verwerking van persoonsgegevens;
- dat de verwerkingsactiviteiten van het LIMC noch opgenomen zijn in Register van verwerkingsactiviteiten Defensie noch het DPIA proces hebben doorlopen;

Besluit;

Op basis van voorgaande overwegingen heb ik op grond van artikel 39 Avg en artikel 1.5 Regeling Avg Defensie besloten op een zo kort mogelijke termijn een Toezichtbezoek uit te voeren bij het LIMC.

3 "Leger verzamelde data in Nederland" en "hoe defensie de eigen bevolking in de gaten houdt" (www.nrc.nl)
4 "land Information Manoeuvre Centre helpt Defensie anticiperen" (www defensie.nl)

DEPARTEMENTAAL VERTROUWELIJK

DEPARTEMENTAAL VERTROUWELIJK

Het toezichtbezoek aan het LIMC is in beginsel gericht op de volgende onderzoeksdoelen:

Bestuursstaf
Directoraat Generaal Beleid
Directie Beleid & Evaluatie
Functionaris Gegevensbescherming

Datum
18-11-2020

Onze referentie
BS2020023515

- Vast te stellen of door het LIMC persoonsgegevens zijn of worden verwerkt zoals bedoeld in de artikelen 2, 4 lid 1 en lid 2 Avg.
- Vast te stellen of door het LIMC bijzondere categorieën van persoonsgegevens zijn of worden verwerkt zoals bedoeld in artikel 9 Avg, waaronder gegevens betreffende de gezondheid en gegevens betreffende politieke, religieuze of levensbeschouwelijke overtuiging.
- Vast te stellen of de verwerking op een rechtmatige grondslag gebaseerd is zoals omschreven in artikel 6 en 9 Avg.
- Vast te stellen of en zo ja welke personen onder het gezag of in opdracht van het LIMC persoonsgegevens verwerken of hebben verwerkt en op welke wijze de logging, autorisatie en toegang tot geautomatiseerde systemen en gegevensbronnen is ingericht.
- Vast te stellen of de verwerkingsactiviteiten van het LIMC dienen te worden opgenomen in het Avg verwerkingenregister Defensie.
- Vast te stellen er een DPIA vereist is.
- Vast te stellen welke technische en organisatorische maatregelen zijn getroffen ter beveiliging van de verwerking zoals bedoeld in artikel 32 Avg en het Defensie beveiligingsbeleid (DBB).

U en uw ondercommandanten worden geacht alle medewerking te verlenen aan de uitvoering van het toezicht.
Voor de volledigheid wijs ik hierbij op het volgende:

- Artikel 38 lid 2 Avg bepaalt dat de FG door de verwerkingsverantwoordelijke wordt ondersteund bij de vervulling van toezichtstaken onder meer door de FG toegang te verschaffen tot de persoonsgegevens en verwerkingsactiviteiten. Zodat de FG kan onderzoeken welke verwerkingsactiviteiten plaatsvinden en of deze voldoen aan de vereisten van de Avg.
- Artikel 1.5 lid 4 van de Regeling Avg Defensie bepaalt dat de FG voor de uitoefening van het toezicht zoals bedoeld in artikel 39 lid 1 b Avg, beschikt over de bevoegdheden van Titel 5.2. van de Algemene Wet Bestuursrecht (Awb). Titel 5.2 van de Awb omvat een brede verzameling van onderzoeksbevoegdheden zoals het betreden van plaatsen, het vorderen van inlichtingen, het onderzoeken van zaken en het kopiëren van bescheiden.
- Artikel 1.5 lid 5 van de Regeling Avg Defensie bepaalt dat een ieder die werkzaam is onder het gezag van de Minister van Defensie verplicht is alle medewerking te verlenen die de FG redelijkerwijze kan vorderen bij de uitoefening van zijn bevoegdheden, tenzij een geheimhoudingsplicht uit hoofde van een wettelijke voorschrift daaraan in de weg staat.

DEPARTEMENTAAL VERTROUWELIJK

DEPARTEMENTAAL VERTROUWELIJK

Bij het onderzoek zal ik mij waar nodig laten ondersteunen door anderen functionarissen bijvoorbeeld vanuit de Beveiligings Autoriteit Defensie.

Naar aanleiding van het toezichtbezoek zal een rapport met conclusies en aanbevelingen worden opgesteld ten behoeve van de Minister als verwerkingsverantwoordelijke en ten behoeve van u als Avg-beheerder.

FUNCTIONARIS GEGEVENSBESCHERMING AVG DEFENSIE

Mevr. mr. O.L. Stenhuis-Kok

Bestuursstaf
Directoraat Generaal Beleid
Directie Beleid & Evaluatie
Functionaris Gegevensbescherming

Datum
18-11-2020

Onze referentie
BS2020023515

Bijlage II: Enquêtevragen

1. **Heeft u in jaar 2020 werkzaamheden verricht voor het LIMC?**
   ja
   nee → door naar vraag 12

2. **Hoelang heeft u <u>in totaal</u> werkzaamheden verricht voor het LIMC?**
   a. minder dan 1 week
   b. een week
   c. tussen 1 week en 1 maand
   d. tussen 1 maand en 3 maanden
   e. langer dan 3 maanden

3. **In welke maand(en) van dit jaar heeft u de werkzaamheden verricht? (meerdere antwoorden mogelijk)**
   - maart
   - april
   - mei
   - juni
   - juli
   - augustus
   - september
   - oktober
   - november

4. **Hieronder volgt een aantal stellingen.**
   Kunt u bij elk van deze stellingen aangeven of ze op uw <u>hoofdtaak</u> binnen LIMC van toepassing waren?

	ja	nee	weet ik niet	wil ik niet zeggen
Heeft u een inwerkprogramma gehad?	O	O	O	O
Waren uw opdrachten helder voor u?	O	O	O	O
Had u een vast aanspreekpunt voor vragen over uw opdrachten?	O	O	O	O
Heeft u een briefing bijgewoond over privacy en de Algemene verordening gegevensbescherming (Avg)?	O	O	O	O
Heeft u een briefing bijgewoond over informatiebeveiliging (security)?	O	O	O	O

Werd er tijdens deze briefings gesproken over de grondslag van het optreden in het civiele en digitale domein?	O	O	O	O
Had u de beschikking over documenten over de Avg?	O	O	O	O
Had u de beschikking over een taakomschrijving?	O	O	O	O

	nooit	**soms**	**noch soms, noch vaak**	**vaak**	**heel vaak**	**wil ik niet zeggen**
Heeft u kennis genomen van de informatiebeveiliging zoals deze is vastgelegd in het Defensie beveiligingsbeleid (DBB)?	O	O	O	O	O	O
Werd er overlegd over uw taken en de uitvoering van deze taken?	O	O	O	O	O	O

Onder een "persoonsgegeven" wordt verstaan: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent, dat informatie ofwel direct over iemand gaat ofwel naar deze persoon te herleiden is (artikel 4 onder 1 Avg).

5. **Hoe vaak bent u voor uw werkzaamheden voor het LIMC in aanraking gekomen met persoonsgegevens?**
   a. nooit → naar vraag 12
   b. soms
   c. noch soms, noch vaak
   d. vaak
   e. heel vaak
   f. wil ik niet zeggen

Onder een "publiek figuur" wordt verstaan: alle personen die politieke of maatschappelijke verantwoordelijkheid dragen, bekende Nederlanders, en anderen die zich in het publieke debat mengen.

6. **a. Op welke categorie personen hebben deze persoonsgegevens betrekking?**
   a. politici/bestuurders
   b. journalisten
   c. wetenschappers
   d. influencers
   e. belangengroepen (woordvoerders)
   f. zorgmedewerkers
   g. defensiemedewerkers
   h. politie/brandweer
   i. anders, namelijk ...

   b. In welke mate hebben deze persoonsgegevens betrekking op publieke figuren?
   a. nooit
   b. soms
   c. noch soms, noch vaak
   d. vaak
   e. heel vaak
   f. weet ik niet / wil ik niet zeggen

7. **Hoe vaak kwam u in aanraking met artikelen waarin een naam vermeld staat?**
   a. nooit
   b. soms
   c. noch soms, noch vaak
   d. vaak
   e. heel vaak
   f. weet ik niet / wil ik niet zegge

   Welk type persoonsgegevens betreft het? (meerdere antwoorden mogelijk)
   De Avg kent drie typen van persoonsgegevens. Onderscheid wordt gemaakt tussen gewone, bijzondere en strafrechtelijke persoonsgegevens.

   a. gewone persoonsgegeven: *zijn gegevens waar een persoon mee kan worden geïdentificeerd.*
   b. bijzondere persoonsgegevens: *zijn gevoelige persoonsgegevens zoals ras, godsdienst of gezondheid.*
   c. strafrechtelijke persoonsgegevens: *zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten. Of met veiligheidsmaatregelen die daarmee verband houden.*
   d. weet ik niet / wil ik niet zeggen

   Indien a, b of c : welke persoonsgegevens betreft het?

   Gewone persoonsgegevens:
   a. naam
   b. adres en woonplaats
   c. telefoonnummer
   d. werknemer-ID
   e. e-mailadres
   f. IP-adres
   g. foto's en video opnamen
   h. anders: namelijk ...

Bijzondere persoonsgegevens:
a. religieuze of levensbeschouwelijke overtuigingen
b. ras/etnische afkomst (denk ook aan pasfoto)
c. politieke opvattingen
d. gezondheid
e. seksueel gedrag/gerichtheid
f. lidmaatschap van een vakbond (denk ook aan contributie)
g. strafrechtelijke veroordelingen en strafbare feiten
h. genetische gegevens (bijv. DNA)
i. biometrische gegevens (bijv. vingerafdruk)
j. burgerservicenummer (BSN)
k. anders, namelijk ...

Strafrechtelijke gegevens:
- Het betreft veroordelingen en verdenkingen van strafbare feiten.
- weet ik niet / wil ik niet zeggen
  open tekstvak

8. **Heeft u naast de bedrijfspagina's/groepen op Facebook ook andere pagina's op Facebook of andere sociale media geraadpleegd?**
   ja/nee/wil ik niet zeggen

   Zo ja, welke waren dit?
   a. Twitter
   b. Instagram
   c. Whatsapp
   e. LinkedIn
   f. Persoonlijke Facebook
   g. Messenger
   h. anders, namelijk ...

9. **Op welke manier kwam u in aanraking met persoonsgegevens en waartoe gebruikte u de deze gegevens? (meerdere antwoorden mogelijk)**
   a. raadplegen
   b. opvragen
   c. verzamelen
   d. opslaan
   e. ordenen / structureren
   f. analyseren en verwerken
   g. bestanden samenvoegen
   h. anonimiseren
   i. verwijderen/wissen
   j. verstrekken
   k. doorzending/verspreiding intern defensie
   l. doorzending/verspreiding extern defensie
   m. wil ik niet zeggen

10. **Is gecontroleerd op de aanwezigheid van persoonsgegevens in de door u opgeleverde (deel)producten?**

    ja/nee/weet ik niet

11. **Waar binnen het LIMC heeft u werkzaamheden uitgevoerd? (meerdere keuzes mogelijk)**
    a. Integrale analyse cell (team 1 Covid ontwikkeling)
    b. Integrale analyse cell (team 2 Desinformatie)
    c. Collection & Engagement
    d. Design & Development
    e. Data OPS
    f. CMD
    g. Plans & Effects
    h. CD&E
    i. anders, namelijk: ....
    j. wil ik niet zeggen

Tot slot. Met deze gegevens wordt vertrouwelijk omgegaan. In de rapportage zullen geen individuen herkenbaar zijn. We rapporteren niet over groepen kleiner dan 10 personen.

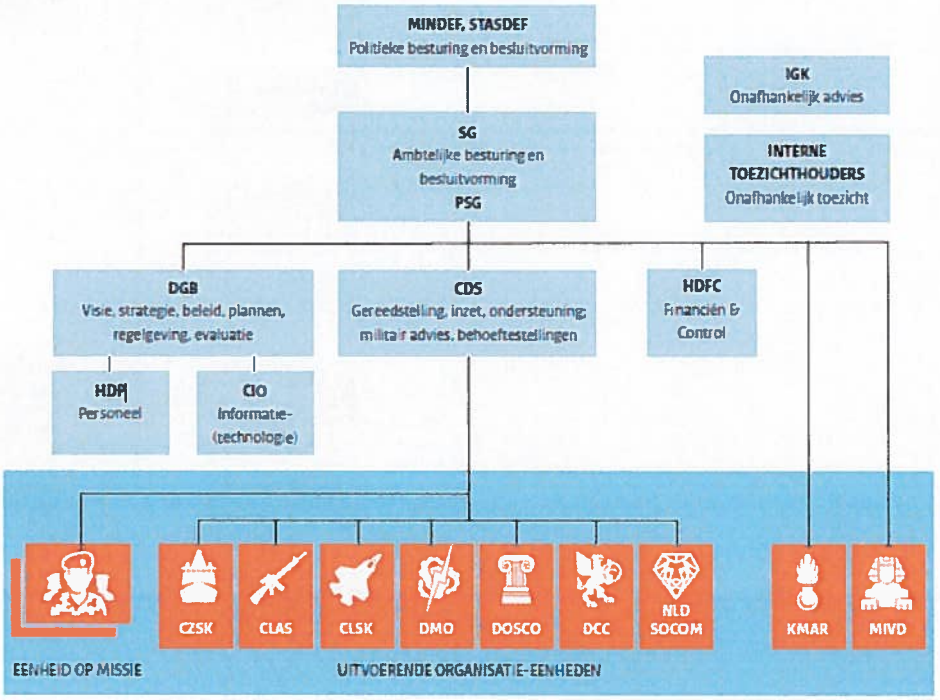
12. **Wilt u nog iets toevoegen aan uw antwoorden of informatie geven over onderwerpen die niet in deze vragenlijst aan bod zijn gekomen?**
    Open tekst vak

13. **Wilt u meewerken aan een interview vul dan hieronder uw e-mailadres in. Afhankelijk van het aantal reacties hierop zullen we u benaderen.**
    Ruimte voor emailadres

Ik heb geen werkzaamheden uitgevoerd voor het LIMC maar heb contact gehad met ... (meerdere keuzes mogelijk)

a. Integrale analyse cell (team 1 Covid ontwikkeling)
b. Integrale analyse cell (team 2 Desinformatie)
c. Collection & Engagement
d. Design & Development
e. Data OPS
f. CMD
g. Plans & Effects
h. CD&E
i. anders, namelijk: ....
j. wil ik niet zeggen

Bijlage III: Organogram Defensie, Koninklijke Landmacht, OOCL



Figuur 12: Schematische weergave hoofdstructuur Defensie[80]

[80] Besturen bij Defensie, 9 februari 2021.

Figuur 13: Organogram Koninklijke Landmacht[81]

Operationeel Ondersteuningscommando Land (OOCL)

Het OOCL bestaat uit onderstaande eenheden:

- Command & Control Ondersteuningscommando
- 101 Geniebataljon
- 400 Geneeskundig Bataljon
- 1 Civiel en Militair Interactiecommando
- Bevoorrading en Transport Commando
- Explosieven Opruimingsdienst Defensie
- Joint ISTAR Commando
- Ondersteuningsgroep CLAS
- Vuursteun Commando

Zie voor een nadere toelichting en een video van het OOCL:
https://www.defensie.nl/organisatie/landmacht/eenheden/oocl

[81] https://www.defensie.nl/organisatie/landmacht/organisatiestructuur.

Bijlage IV: Analyseresultaten rapportages LIMC

De ontvangen *output*-rapportages van het LIMC die zijn verspreid in de periode 23 maart 2020 tot en met 27 november 2020 zijn geanalyseerd op de verwerking van persoonsgegevens. De analyse was gericht op vermelding (de verwerking) van (bijzondere) persoonsgegevens.

Conclusie

Op basis van aangetroffen persoonsgegevens in de *output*-rapportages is er geen aanwijzing dat er sprake is geweest van een grootschalige en gerichte verwerking van (bijzondere) persoonsgegevens. Uit rapportanalyse blijkt dat namen en functies, van met name publieke personen, voorkomen. Deze zijn afkomstig uit openbare nieuwsbronnen en bronvermeldingen. De gebruikte persoonsgegevens zijn voornamelijk verbonden aan een bepaald narratief, zoals 'Virusnarratief' of 'Vaccinatienarratief'. Aan deze narratieven zijn bepaalde personen (namen/functies) verbonden, die door het LIMC genoemd zijn in de rapportages. Daarbij ging het om de ontwikkeling van het narratief.

De rapportages van het LIMC laten in de periode van maart/mei tot en met november 2020 een ontwikkeling zien. Van dagelijkse rapporten over de statistische ontwikkelingen rondom COVID-19 en de ontwikkelingen rond bepaalde 'narratieven' in de media, naar het produceren van wekelijkse rapportages over de statistische ontwikkelingen van de COVID-19 pandemie en narratieven over desinformatie rondom COVID-19, welke speelden in de samenleving en in de media.

Beide typen rapportages zijn onderzocht op de verwerking van persoonsgegevens.

Onderzochte rapportages op persoonsgegevens

In totaal heeft het onderzoeksteam 80 rapportages geanalyseerd op de verwerking van (bijzondere) persoonsgegevens.

In 34 rapportages zijn persoonsgegevens verwerkt. Deze informatie is deels direct herleidbaar tot een natuurlijk persoon op basis van een persoonsnaam en deels indirect herleidbaar bijvoorbeeld op basis van functieaanduiding.

De bronvermeldingen betreft persoonsgegevens die in oorspronkelijke, openbaar toegankelijke documenten of teksten, zijn gebruikt, waarnaar het LIMC een verwijzing (vermelding) doet. Behalve de namen of functies van de personen gaat dit ook om informatie betreffende de sociale en maatschappelijke context. Bijvoorbeeld een naam van een natuurlijke persoon wordt volgens een krantenartikel in verband gebracht met bepaalde feiten, beweringen of meningen over het COVID-19 virus.

In onderstaande tabel staat vermeld in hoeveel rapporten persoonsgegevens van een betrokkene voorkomen en of een naam/functie in de inhoud of in de bronvermelding voorkomt.

Betrokkenen	Aantal rapporten waarin betrokkene voorkomt	In inhoud van rapport	In bronvermelding van rapport
betrokkene 1	21	Ja	Ja
betrokkene 2	7	Ja	Ja
betrokkene 3	5	Ja	Ja
betrokkene 4	4	Ja	Ja
betrokkene 5	4	Ja	Ja
betrokkene 6	4	Ja	Ja
betrokkene 7	4		Ja
betrokkene 8	3	Ja	Ja
betrokkene 9	3	Ja	Ja
betrokkene 10	2		Ja
betrokkene 11	2	Ja	Ja
betrokkene 12	2	Ja	Ja
betrokkene 13	2		Ja
betrokkene 14	2		Ja
betrokkene 15	2		Ja
betrokkene 16	2	Ja	
betrokkene 17	2		Ja
betrokkene 18	1	Ja	
betrokkene 19	1		Ja
betrokkene 20	1		Ja
betrokkene 21	1	Ja	
betrokkene 22	1		Ja
betrokkene 23	1		Ja
betrokkene 24	1		Ja
betrokkene 25	1	Ja	
betrokkene 26	1		Ja
betrokkene 27	1		Ja
betrokkene 28	1		Ja
betrokkene 29	1		Ja
betrokkene 30	1		Ja
betrokkene 31	1	Ja	
betrokkene 32	1		Ja
betrokkene 33	1	Ja	
betrokkene 34	1		Ja
betrokkene 35	1	Ja	
betrokkene 36	1	Ja	
betrokkene 37	1		Ja
betrokkene 38	1	Ja	
betrokkene 39	1	Ja	
betrokkene 40	1		Ja

Betrokkenen	Aantal rapporten waarin betrokkene voorkomt	In inhoud van rapport	In bronvermelding van rapport
betrokkene 41	1	Ja	
betrokkene 42	1		Ja
betrokkene 43	1		Ja
betrokkene 44	1		Ja
betrokkene 45	1		Ja
betrokkene 46	1	Ja	
betrokkene 47	1	Ja	
betrokkene 48	1		Ja
betrokkene 49	1		Ja
betrokkene 50	1		Ja

Tabel 11: Detailanalyse rapporten

Bijlage V: Verdieping toetsingskader

Verwerkingsverantwoordelijke

Een verwerkingsverantwoordelijke is degene die, alleen of samen met anderen, het doel en de middelen van de verwerking van persoonsgegevens vaststelt.[82]

Met het bepalen van het doel van de verwerking wordt bedoeld dat de verwerkingsverantwoordelijke de zeggenschap heeft over waarom de persoonsgegevens worden verwerkt en voor welke concrete doelen de persoonsgegevens zullen worden ingezet. Het vaststellen van het doel van de verwerking is een exclusieve bevoegdheid van de verwerkingsverantwoordelijke.

Met het vaststellen van de middelen van de verwerking wordt gedoeld op het vaststellen van de wijze waarop de verwerking plaats zal vinden, kortom: hoe worden de persoonsgegevens verwerkt ten behoeve van het vastgestelde doel.

Het is eveneens mogelijk dat in de bijzondere wetten uitdrukkelijk is bepaald wie verwerkingsverantwoordelijke is voor de persoonsgegevens die op grond van de betreffende wet mogen worden verwerkt.

Verwerker

De verwerker is degene die ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.[83] De verwerker ontleent zijn bevoegdheid om persoonsgegevens te verwerken aan de bevoegdheid van de verwerkingsverantwoordelijke die hem inschakelt. De bevoegdheden van een verwerker moeten zijn vastgelegd in een verwerkersovereenkomst.[84]

Kenmerkend voor een verwerker is dat de verwerker:

- een externe natuurlijke persoon, rechtspersoon, overheidsinstantie, dienst of orgaan is, die geen onderdeel vormt van de organisatie van de verwerkingsverantwoordelijke, en;
- persoonsgegevens voor de verwerkingsverantwoordelijke verwerkt, op diens instructies en onder diens verantwoordelijkheid – en dus niet voor zichzelf.[85]

Voor de kwalificatie van verwerker is bepalend of de partij aanwijzingen van de verwerkingsverantwoordelijke dient op te volgen met betrekking tot de verwerking van persoonsgegevens. Zo ja, dan is de partij een verwerker. Uitgangspunt is dat de verwerker niet mag afwijken van de afspraken die in de verwerkersovereenkomst met de verwerkingsverantwoordelijke zijn gemaakt. Dat betekent overigens niet dat de verwerker op detailniveau aanwijzingen van de verwerkingsverantwoordelijke moet ontvangen en volgen over de gegevensverwerking, maar (in ieder geval) wel

---

[82] Artikel 4, aanhef en onder 7, Avg.
[83] Artikel 4, aanhef en onder 8, Avg.
[84] Artikel 28, derde lid, Avg.

[85] Op het moment dat een verwerker verwerkingen voor zichzelf (of in strijd met de instructies van de verwerkingsverantwoordelijke) verricht, en aldus feitelijk handelt als verwerkingsverantwoordelijke, zal de verwerker (voor dat deel) worden aangemerkt als verwerkingsverantwoordelijke.

voor zover het gaat om het doel van de verwerking en de wezenlijke aspecten van de middelen voor de verwerking.[86]

Gepseudonimiseerde en geanonimiseerde gegevens

De Artikel 29-Werkgroep (inmiddels opgegaan in: de *European Data Protection Board* ("EDPB")) – waarin de Europese privacytoezichthouders zijn verenigd – geeft in haar richtlijnen en adviezen aan dat pas gesproken kan worden van 'anonieme gegevens' indien iedere mogelijkheid tot identificatie van de betrokkene onherroepelijk is uitgesloten.[87] Daarbij neemt de Artikel 29-Werkgroep tot uitgangspunt dat herleidbaarheid, koppelbaarheid en deduceerbaarheid onmogelijk moet zijn.[88] Onvoldoende in dat verband is het wissen van namen of het vervangen van dergelijke gegevens met willekeurige andere gegevens.

Zelfs de geavanceerde versleuteling en/of hashing van persoonsgegevens is in dat kader, volgens de Europese privacytoezichthouders veelal onvoldoende en dient te worden gezien als een manier om persoonsgegevens te pseudonimiseren, zoals bedoeld in artikel 4, onder 5, Avg en geldt dus als een beveiligingsmaatregel.[89] Reden daarvoor is volgens de Artikel 29-Werkgroep dat – anders dan bij anonimisering, waarbij *elke* mogelijkheid tot identificatie onomkeerbaar wordt uitgesloten – bij pseudonimisering de kans op identificatie blijft bestaan. De inzet van pseudonimisering heeft enkel tot gevolg dat de koppelbaarheid van een dataset aan de oorspronkelijke dataset wordt *beperkt*. Degene die versleuteling en/of hashing heeft toegepast, houdt echter de beschikking over de encryptiesleutel en/of de oorspronkelijke gegevens. Gepseudonimiseerde persoonsgegevens vallen daarmee onverkort onder de reikwijdte van de Avg.[90]

Hergebruik persoonsgegevens gepubliceerd op internet

Het voorgaande is ook van betekenis voor het hergebruik van persoonsgegevens die zijn gepubliceerd op het internet. Deze gegevens zijn immers voor bepaalde doeleinden openbaar gemaakt en kunnen niet zomaar worden hergebruikt.

Zo overweegt de Autoriteit Persoonsgegevens het volgende op haar website[91] over hergebruik van op het internet gepubliceerde gegevens:
"Veel mensen gebruiken gegevens van andere websites voor een eigen publicatie op internet. Bijvoorbeeld foto's waar mensen herkenbaar op staan of adressen. Dat deze gegevens al op internet staan, betekent echter niet dat iemand ze zomaar

---

[86] Zie Artikel 29-Werkgroep, 'Advies 1/2010 over de begrippen "voor de verwerking verantwoordelijke" en "verwerker"', 16 februari 2010, p. 29.
[87] In deze groep waren (tot en met 25 mei 2018) de Europese privacytoezichthouders verenigd. De groep bracht onder meer adviezen uit over de interpretatie van begrippen in de Privacyrichtlijn (Richtlijn 95/46/EG) en de Wbp. De opinies van deze groep waren en zijn nog steeds zeer gezaghebbend. Sinds 25 mei 2018 heeft de EDPB de taken van de Artikel 29-Werkgroep overgenomen. De eerdere adviezen van de Artikel 29-Werkgroep zijn door de EDPB bekrachtigd.
[88] Zie Artikel 29-Werkgroep, 'Advies 5/2014 over anonimiseringstechnieken', WP 216, p. 24.
[89] Zie Artikel 29-Werkgroep, 'Advies 5/2014 over anonimiseringstechnieken', WP 216, p. 1. Zie ook artikel 32, eerste lid, aanhef en onder a, Avg.
[90] Zie verder overweging 26 en 28 van de considerans van de Avg.
[91] Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internet-telefoon-tv-en-post/persoonsgegevens-op-internet.

opnieuw mag gebruiken. De gegevens worden dan namelijk in een andere context gebruikt en voor een ander doel."

Verdere verwerking ziet in de verordening op verwerkingen van persoonsgegevens voor een ander doel dan waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Dit kan verwerking door één en dezelfde verwerkingsverantwoordelijke zijn, maar de verdere verwerking kan ook de verstrekking van gegevens aan een andere verwerkingsverantwoordelijke inhouden.

De verwerkingsverantwoordelijke die persoonsgegevens ontvangt, zal voor de verwerking van de ontvangen gegevens een zelfstandige rechtsgrondslag nodig hebben als bedoeld in artikel 6, eerste lid, van de verordening bijvoorbeeld dat de verwerking noodzakelijk is voor de uitoefening van de taak van algemeen belang[92].

Indien sprake is van een verenigbare verdere verwerking, dan is bij een interne verdere verwerking (door dezelfde verwerkingsverantwoordelijke) geen afzonderlijke wettelijke grondslag als bedoeld in artikel 6, eerste lid, Avg vereist. Bij een externe verdere verwerking (door een andere verwerkingsverantwoordelijke) dient de verwerkingsverantwoordelijke over een afzonderlijke wettelijke grondslag als bedoeld in artikel 6, eerste lid, Avg te beschikken. Doordat het bij gebruik door het LIMC veelal zal gaan om de verdere verwerking na een verstrekking, zal de verwerkingsverantwoordelijke een eigen grondslag nodig hebben om de ontvangen gegevens te verwerken. Zie *Kamerstukken II* 2018/19, 34 851, nr. 3, p. 38.[93]

Bijzondere en strafrechtelijke gegevens

De bijzondere persoonsgegevens en strafrechtelijke persoonsgegevens zijn persoonsgegevens die naar hun aard gevoelig zijn en waarvoor de Avg aanvullende regels stelt.

De bijzondere categorieën van persoonsgegevens zijn limitatief opgesomd in artikel 9, eerste lid, Avg, daaronder vallen bijvoorbeeld gegevens over iemands politieke opvattingen, ras, gezondheid, religie of gegevens met betrekking tot iemands seksueel gedrag.[94] Een dergelijke bijzondere categorie kan direct door het persoonsgegeven worden onthult, maar ook indirect. In dat verband is het wel nodig, zoals de Nederlandse wetgever opmerkt bij de toelichting op de UAvg,[95] dat er een rechtstreeks verband is. Gegevens die slechts een indicatie geven dat het om een bijzonder categorie zou kunnen gaan, vallen buiten de reikwijdte van artikel 9 Avg.[96]

Ras of etnische afkomst

De Autoriteit Persoonsgegevens merkt inzake de verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag, en de vraag of dat een verwerking van een (indirect) bijzonder persoonsgegeven betreft, het volgende op:[97]

---

[92] Zie *Kamerstukken II* 2018/19, 34851, nr. 3 p.37.

[93] Deze opmerking in de memorie van toelichting is toegevoegd naar aanleiding van het wetgevingsadvies van de Afdeling advisering van de Raad van State (*Kamerstukken II* 2017/18, 34 851, nr. 4, p. 36-38).

[94] Vgl. artikel 4, aanhef en onder 13, Avg jo. artikel 9, eerste lid, Avg.

[95] Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 33 e.v.

[96] Zie ook 'Bijlage 1 Zienswijze Facebook Inc. en Facebook Ierland van 16 september 2015 met reactie Autoriteit Persoonsgegevens', 21 februari 2017, z2014-00929.

[97] Autoriteit Persoonsgegevens, 'Belastingdienst/Toeslagen – De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag' van 17 juli 2020, z2018-22445 (raadpleegbaar via:

"Uit Nederlandse rechtspraak volgt dat in het kader van nationaliteit ook belang toekomt aan de overige verwerkte persoonsgegevens. Indien nationaliteit wordt verwerkt in combinatie met bijvoorbeeld geboorteland, geboorteplaats, herkomst en/of pasfoto wordt in rechtspraak aangenomen dat er wel sprake is van gegevens waaruit het ras of de etnische afkomst blijkt.[98] Aanvullend kan de context van de verwerking er in bepaalde gevallen toe leiden dat nationaliteit op zichzelf toch aangemerkt kan worden als bijzonder persoonsgegeven. De AP beschouwt nationaliteit als bijzonder persoonsgegeven wanneer de verwerking tot doel heeft om onderscheid te maken naar ras of etnische afkomst, of indien het voor de verwerkingsverantwoordelijke redelijkerwijs voorzienbaar is dat de verwerking tot het maken van onderscheid naar ras of etnische afkomst zal leiden."

De Autoriteit Persoonsgegevens verwijst in dat verband naar *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 106:

"Indien een school bij voorbeeld met het oog op de identificatie van de leerlingen van hen allen de geboorteplaats in de administratie opneemt, vloeit uit deze verwerking, indien het gaat om de geboorteplaats in het buitenland, niet rechtstreeks een gevoelig gegeven voort. De verwerking heeft niet plaats gevonden met het doel om de mogelijk andere etnische herkomst van de leerlingen te registreren. Dit laat de mogelijkheid open dat dergelijke gegevens, mogelijk door vergelijking met andere gegevens, alsnog worden gebruikt om gegevens omtrent ras te herleiden."

Gegevens over gezondheid

In het kader van de beoordeling van de activiteiten binnen het LIMC komt vooral betekenis toe aan de bijzondere categorie gezondheid, levensovertuiging en politieke gezindheid. Het begrip gezondheidsgegevens wordt ruim uitgelegd.[99] Zo kan volgens de EDPB informatie wegens het gebruik ervan in een specifieke context, waaronder bijvoorbeeld een recente reis of verblijf in een door COVID-19 getroffen regio die bij het stellen van een diagnosis is verwerkt door een zorgverlener, of informatie uit een op zelfcontrole gebaseerde vragenlijst, waarbij betrokkenen vragen over hun gezondheid beantwoorden, reeds kwalificeren als gegevens over gezondheid.[100]

Politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen

De begrippen levensovertuiging en politieke gezindheid, dienen uitgelegd te worden overeenkomstig artikel 1 Grondwet en de Algemene wet gelijke behandeling. Het begrip politieke gezindheid duidt op een gemeenschappelijke opvatting omtrent de bestuurlijke en sociale inrichting van de samenleving en het begrip

---

https://www.autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/onderzoek_belastingdienst_kinderopvangtoeslag.pdf), p. 35 en 36.

[98] Zie bijvoorbeeld HR 13 juni 2000, ECLI:NL:HR:2000:AA6191.

[99] Zie bijvoorbeeld HvJ EU van 6 november 2003, ECLI:EU:C:2003:596, C-101/01 (*Lindqvist*), par. 50.

[100] Zie EDPB, 'Richtsnoeren 3/2020 inzake de verwerking van gezondheidsgegevens voor wetenschappelijk onderzoek in het kader van de COVID-19-uitbraak', 21 april 2020 (raadpleegbaar via: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_nl.pdf), p. 5.

levensovertuiging op een gemeenschappelijke fundamentele opvatting over de samenleving en het menselijk bestaan.[101]

Strafrechtelijke gegevens

Wat moet worden verstaan onder strafrechtelijke persoonsgegevens, zoals bedoeld in artikel 10 Avg, is niet geheel duidelijk. Hetzelfde geldt voor het (ruimere) door de Nederlandse wetgever geïntroduceerde begrip uit artikel 1 UAvg: 'persoonsgegevens strafrechtelijke aard'[102], waarover het Gerechtshof Den Haag in haar arrest van 24 december 2019[103] overwoog dat de nationale wetgever niet de mogelijkheid heeft om een eigen, ruimere invulling te geven aan het Unierechtelijk begrip aangezien dat autonoom moet worden uitgelegd.[104]

Aanknopingspunt voor de uitleg van het begrip persoonsgegevens van strafrechtelijke aard en strafrechtelijke persoonsgegevens is te vinden in de parlementaire geschiedenis bij de Wbp.[105] Daarin wordt opgemerkt dat het betrekking heeft op 'zowel op veroordelingen als op min of meer gegronde verdenkingen'. Dit wordt vervolgens op de volgende wijze toegelicht:

"Veroordelingen betreffen gegevens waarbij de rechter, al dan niet onherroepelijk, strafrechtelijk gedrag heeft vastgesteld. Bij verdenkingen gaat het om concrete aanwijzingen jegens een bepaalde persoon. Het begrip strafrechtelijk gegevens omvat mede gegevens omtrent de toepassing van het formele strafrecht, bijvoorbeeld het gegeven dat iemand is gearresteerd of dat tegen hem proces-verbaal is opgemaakt wegens een bepaald vergrijp. De bepaling heeft geen

---

[101] Zie College voor de Rechten van de Mens, 23 februari 2005, nr. 2005-28, rov. 5.4-5.7: "5.5 Volgens vaste jurisprudentie van de Commissie is bij godsdienst sprake van een overtuiging omtrent het leven waarbij een opperwezen centraal staat, terwijl bij een levensovertuiging dit opperwezen ontbreekt, maar er eveneens een dergelijke existentiële gemeenschappelijke overtuiging bestaat (zie CGB 4 februari 1997, oordeel 1997-15). 5.6 Volgens vaste jurisprudentie verstaat de Commissie onder levensovertuiging een min of meer coherent stelsel van ideeën, waarbij het gaat om fundamentele opvattingen over het menselijk bestaan (zie onder meer CGB 4 februari 1997, oordeel 1997-15 en CGB 5 februari 2002, oordeel 2002-04). 5.7 Ook acht de Commissie het noodzakelijk dat deze opvatting niet slechts individueel beleefd wordt, maar dat sprake is van een gemeenschappelijke opvatting (CGB 4 februari 1997, oordeel 1997-15)." (onderstreping toegevoegd). Zie voorts College voor de Rechten van de Mens, 8 maart 2011, nr. 2011-31, rov. 3.10: "Het begrip politieke overtuiging duidt op een gemeenschappelijke opvatting omtrent de bestuurlijke en sociale inrichting van de samenleving. Deze opvatting dient te kunnen worden afgeleid uit een bepaald handelen of nalaten van een persoon (zie: CGB 4 februari 1997, 1997-15, overweging 4.5; CGB 9 juli 2002, 2002-84, overweging 5.5; CGB 18 januari 2005, 2005-3, overweging 5.10 en CGB 21 april 2006, 2006-76, overweging 3.5)." (onderstreping toegevoegd).

[102] Dit begrip omvat tevens 'persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag vallen'.

[103] Zie Gerechtshof Den Haag van 24 december 2019, ECLI:NL:GHDHA:2019:3539, rov. 4.23.

[104] Ook het Gerechtshof Amsterdam signaleert dit punt in de uitspraak van 23 juni 2020, al wordt er in die uitspraak geen inhoudelijk oordeel over gegeven. Zie Gerechtshof Amsterdam 23 juni 2020, ECLI:NL:GHAMS:2020:1802, rov. 2.18: "[...] [geïntimeerde] heeft ter onderbouwing van dit standpunt gewezen op de ruimere definitie van het begrip 'persoonsgegevens van strafrechtelijke aard' in artikel 1 van de Uitvoeringswet Avg (hierna: UAvg). Daargelaten of het de Nederlandse wetgever vrij stond om in artikel 1 van de UAvg een ruimere betekenis dan in de Avg te geven aan dit begrip, overweegt het hof dat ook in geval van strafrechtelijke persoonsgegevens getoetst dient te worden aan artikel 17 lid 3 van de Avg op de wijze zoals is overwogen in het hiervoor genoemde HvJEU GC e.a./CNIL-arrest, r.o. 66-69, en dat de in dat kader te maken belangenafweging, waarbij het gevoelige karakter van strafrechtelijke persoonsgegevens en het belang deze geheim te houden worden onderkend, niet tot een andere uitkomst zou hebben geleid dan hiervoor vermeld."

[105] Deze wetsgeschiedenis is relevant aangezien de wetgever bij de toelichting op de UAvg aangeeft dat voor de uitleg van het begrip aangesloten kan worden bij de uitleg in de Wbp. Zie *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 65 en 90.

betrekking op de verwerking van persoonsgegevens gericht op de vaststelling van mogelijk strafbaar gedrag, bij voorbeeld door het volgen van trends."[106]

Uit de rechtspraak kan verder worden opgemaakt wat onder deze strafrechtelijke gegevens moeten worden verstaan. Het moet gaan om:

"zodanige concrete feiten en omstandigheden dat zij een als strafbaar feit te kwalificeren bewezenverklaring [...] kunnen dragen en [...] of de vastgestelde gedragingen een zwaardere verdenking dan een redelijk vermoeden van schuld [oplevert], in die zin dat de te verwerken strafrechtelijke persoonsgegevens[, dient] in voldoende mate moeten vaststaan." (tekst tussen blokhaken toegevoegd)

Vgl. Hoge Raad 29 mei 2009, ECLI:NL:HR:2009:BH4720, rov. 4.4.[107]

Onder verwijzing naar voornoemde parlementaire geschiedenis en rechtspraak komt de rechtbank Amsterdam in haar uitspraak van 22 maart 2018[108] tot de gevolgtrekking dat er niet snel mag worden aangenomen dat verwerkte gegevens strafrechtelijke persoonsgegevens (en persoonsgegevens van strafrechtelijke aard) zijn. Een beschuldiging is volgens de rechtbank Amsterdam onvoldoende, er moet sprake zijn 'concrete, voldoende zwaarwegende aanwijzingen' van strafbaar gedrag.

Zie Rechtbank Amsterdam 22 maart 2018, ECLI:NL:2018:3357, rov. 4.4-4.5:

"Niet voldoende is dat de betrokkene wordt beschuldigd van strafbaar gedrag. De wetsgeschiedenis en jurisprudentie [..] bieden voldoende aanwijzingen dat het moet gaan om bewezen feiten, of gegronde verdenkingen, dus verdenkingen die zijn onderbouwd met concrete, voldoende zwaarwegende aanwijzingen dat een bepaald persoon zich aan strafbaar gedrag heeft schuldig gemaakt."

Het is niet helemaal duidelijk wat er moet worden volstaan onder de in artikel 10 V en artikel 1 UAvg ook nog genoemde 'daarmee verband houdende veiligheidsmaatregelen' (in het Engels '*related security measures*'). Aannemelijk is echter dat het hier gaat om maatregelen die door een strafrechter, of ten minste in het kader van een strafrechtelijke veroordeling, worden opgelegd, zoals een TBS-maatregel.

---

[106] Zie *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 102 en 118.
[107] Zie meer recent Gerechtshof Arnhem-Leeuwarden 28 maart 2020, ECLI:NL:GHARL:2020:3374, rov. 5.26 en 5.27.
[108] Rechtbank Amsterdam 22 maart 2018, ECLI:NL:2018:3357.

Bijlage VI: Reactie op niet overgenomen punten 'hoor/wederhoor'

Bevinding, geen verwerking bijzondere persoonsgegevens
Dit is niet alleen gebleken uit interviews, het FG team heeft toegang gehad tot alle systemen en informatie. Er zijn geen gegevens verwerkt mbt de gezondheid van personen. Daar was ook de vraagstelling en interesse niet naar, het ging op het kunnen volgen en voorspellen van trends.

Feitelijke onderbouwing. Het onderzoeksteam heeft geen forensisch onderzoek verricht.

Bevinding, tabel met bronnen nr. 11, nr 12, nr 15, nr 21, nr 23, nr 24, nr 29
Betreft interne LIMC (half)producten. In de tabel svp opnemen als LIMC-producten en niet als CLAS producten. Daarnaast adviseren we geen gebruik te maken van de term OSINT.

Aanduidingen CLAS en OSINT zijn conform verstrekt IVP. Detailgegevens over de bron waren al weggelaten.

Bevinding, namen in bronvermeldingen
Het gebruik van namen in bronvermeldingen betrof uitsluitend en alleen een directe overname van een url om de bronvermelding zo zuiver mogelijk te houden. Het was de staande afspraak bronvermelding zo duidelijk mogelijk toe te passen om zo transparant te zijn welke informatie het LIMC gebruikte. Diverse Nederlandse media gebruiken url's waarin een combinatie van het htttp adres plus de kop van het artikel staat vermeld. Dat verklaart de opname van een aantal persoonsnamen in de bronvermelding. Deze nuance is naar onze mening belangrijk om op te nemen in deze paragraaf. Het belang van een correcte bronvermelding in het kader van transparantie stond voorop, in het kader van betrouwbaarheid en herleidbaarheid van de gepresenteerde informatie. Tevens achten we het van belang dat deze duiding terugkomt in de samenvatting en conclusie omdat een naam in een bronvermelding echt iets anders is dan waar gemiddeld genomen aan gedacht wordt bij verwerken van persoonsgegevens. Hiermee werd ook voorkomen dat rapportages zich op verschillende niveaus gingen herbevestigen. (kortom denken dat een bericht uit meerdere bronnen komen, maar eigenlijk het napraten van 1 bron is).

Het gebruik van de namen en functies van politici en bestuurders is nader toegelicht.

Bevinding, tabellen met percentages
De duiding van de percentages ontbreekt, waardoor de vraag blijft hangen of iets 'veel' of 'weinig' is.

Gebruik tabelcijfers is toegelicht.

Bevinding, onderbouwing norm privé laptop
Onduidelijk naar welke norm verwezen wordt, omdat gebruik van privé laptops niet per definitie uitgesloten is binnen Defensie.

De voornaamste normen staan in de beleidsinstructie D/201 – behandelen van informatie.

Op grond van onder andere onderstaande normen kan worden vastgesteld dat met het gebruik van een privé laptop voor het verwerken van gemerkte informatie, niet aantoonbaar wordt voldaan aan het DBB.

- *D/201-140 Gemerkte informatie kan bij kennisname door niet-gerechtigden leiden tot schade aan de belangen van een natuurlijke- of rechtspersoon.*
- *D/201-260 Gerubriceerde en/of gemerkte magnetische harde schijven en Solid State Drives (SSD) die voor hergebruik of afstoting zijn bestemd, moeten worden geschoond door toepassing van het gecertificeerde wisprogramma Blanco Data Cleaner waarbij in de "Modellenatlas" de actuele versie is genoemd. De juiste wijze van gebruik is beschreven in inzetadviezen*
- *D/201-430 Gerubriceerde en/of gemerkte informatie wordt na gebruik in een daartoe aangewezen medium opgeborgen.*
- *D/201-460 Het opslaan of verwerken van gerubriceerde en/of gemerkte informatie mag alleen op geaccrediteerde informatiesystemen.*
- *D/201-470 Het opslaan of verwerken van gerubriceerde en/of gemerkte informatie op een harddisk van een laptop geschiedt te allen tijde met gebruikmaking van een door Defensie goedgekeurd vercijferproduct per rubriceringsniveau. De op deze manieren vercijferde informatie kan alleen dan als ONGERUBRICEERD worden behandeld.*

Alleen ongerubriceerde EN ongemerkte informatie mag op een privé ICT middel worden opgeslagen, mits aan de volgende norm wordt voldaan.

- *Norm*
  D/201-420 Nationaal ongerubriceerde en ongemerkte informatie mag eventueel op privé IT-middelen worden opgeslagen en verwerkt als aan de volgende eisen wordt voldaan:
  - *de privé IT-middelen dienen aan minimale beveiligingseisen te voldoen, zoals toegangswachtwoord, actuele virusscanner en firewall;*
  - *kennisname door niet gerechtigden dient te worden voorkomen;*
  - *alleen een door Defensie goedgekeurde USB-stick mag worden gebruikt;*

Na gebruik dient de betreffende informatie zo spoedig mogelijk van het privé ICT-middel te worden verwijderd.

Bijlage VII: Geraadpleegde documenten

Het onderzoeksteam heeft gebruik gemaakt van de (U)Avg regelgeving en jurisprudentie. Aanvullend aan de vermelde bronnen zijn met name onderstaande documenten geraadpleegd.

- Autoriteit Persoonsgegevens (2017, 6 juni). *Sociale media databases.* Den Haag. z2017-03931
- Autoriteit Persoonsgegevens (2019, 19 november). *Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens.* Den Haag: Staatscourant 64418
- Autoriteit Persoonsgegevens (2020, 17 juli). *Belastingdienst/Toeslagen: De verwerking van de nationaliteit van aanvragers van kinderopvangtoeslag.* Den Haag: onderzoeksrapport z2018-22445
- College Bescherming Persoonsgegevens (2017, december). *CBP richtsnoeren: Publicatie van Persoonsgegevens op internet.* Den Haag
- Directoraat-Generaal Justitie van de Europese Commissie (2017, 4 oktober). *Richtsnoeren voor gegevensbeschermingseffectbeoordelingen en bepaling of een verwerking "waarschijnlijk een hoog risico inhoudt" in de zin van Verordening 2016/679.* Brussel: Groep gegevensbescherming artikel 29
- European Data Protection Board (2020, 2 september). *Guidelines 8/2020 on the targeting of social media users Version 1.0*
- Ministerie van Buitenlandse Zaken (2020, 16 november). *Internationale rechtsorde in het digitale domein.* Den Haag: Directie Veiligheidsbeleid
- Ministerie van Defensie (2011, 21 mei). *Aanwijzing SG A/990: Handboek militaire ondersteuning civiele autoriteiten.* Den Haag: SG
- Ministerie van Defensie (2020, 11 maart). *OPERATIEBEVEL NR 2020/710 (COVID-19).* Utrecht: Commandant Landstrijdkrachten. *CLAS2020003483*
- Ministerie van Defensie (2020, 20 augustus). *OPERATIEBEVEL 2020-8154 (200814 MSOB INTERDEP ONDERSTEUNEN VWS (COVID-19).* Utrecht: Staf Clas/Directie Training en Operaties. *2020016580*
- Ministerie van Defensie (2020, 24 augustus). *Beveiligingsplan JISTARC.* 't Harde: JISTARC. *Versienummer 2020-01*
- Ministerie van Defensie (2020, 24 september). *voortgangsverslag 2_ CDE_LIMC.* 't Harde: LIMC. *Experimenten LIMC: Thema's, Activiteiten en Experimenten om Relevant en Dominant te zijn in het Informatiedomein*
- Ministerie van Defensie (2020, 5 oktober (laatste update)). *Informatieverzamelplan 20200721-DV-LIMC-IVP.* 't Harde: LIMC
- Ministerie van Defensie (2020, 23 november). *Fiche_LIMC_vgeintegreerd_vJ: Tijdlijn ontwikkeling LIMC.* C-LIMC
- Ministerie van Defensie (2020, 24 november). *Presentatie OSINT Proces/werkwijze.* 't Harde: 109 OSINT. *24112020-DV-109OSINT*
- Ministerie van Defensie (2020, 27 november). *Reactie op NRC-artikel van 15 november over LIMC.* Den Haag: Minister. *BS2020024149*
- Ministerie van Defensie (2020, 27 oktober). *Beleidstoets Interim Architectuur LIMC: Projectkaart.* Utrecht: Staf Clas/Afdeling Strategie en Plannen
- Ministerie van Defensie (2020, 28 mei). *WEB_202050528_Clas Visie IGO_A4 Brochure.* Koninklijke Landmacht. *Visie Informatiegestuurd voor de Landmacht: Manoeuvreren in de Informatieomgeving*

- Ministerie van Defensie (2020, 3 november). *20200311_DV_STAFCLAS-DTenO_Operatieorder-2020-710.* Utrecht: Staf Clas/Directie Training en Operaties
- Ministerie van Defensie (2020, 8 juni). *CD-E voortgangsverslag LIMC 200608.* 't Harde: LIMC. *Experimenten LIMC: Thema's, Activiteiten en Experimenten om Relevant en Dominant te zijn in het Informatiedomein*
- Ministerie van Defensie (2020, april). *FRAGO 004 (LAND INFORMATION MANOEUVRE CENTRED BI3 OPERATIEBEVEL NR 2020-039 (RESILIENCE CQVID-191.* Apeldoorn: C-OOCL. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2020, februari). *OPERATIEBEVEL NR 2020-25 (COVID-19).* Apeldoorn. C-OOCL. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2020, juni). *FRAGO 011 (VOORTZETTING LIMC) BIJ OPERATIEBEVEL NR 2020-039 (RESILIENCE COVID-19).* Apeldoorn: C-OOCL. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2020, maart). *FRAGO 001 BIJ OPERATIEBEVEL NR 2020-025 (COVID-19).* Apeldoorn: C-OOCL. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2020, maart). *OPERATIEBEVEL NO. 2020-001 (COVID-19)*
  't Harde: C-JISTARC. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2020, mei). *FRAGO 009 (VULLING LIMC) BIJ OPERATIEBEVEL NR 2020-039 (RESILIENCE COVID-19).* Apeldoorn: C-OOCL. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2020, november). *20201123-DV-LIMC_ mediaenwebcarerapportage_aanpak opdrachten: Media & Webcare RAPPORT 001.* LIMC. *Departementaal Vertrouwelijk*
- Ministerie van Defensie (2021, 21 januari). *20210121 Commandanten appreciatie LIMC.* Utrecht: Staf Clas/Kabinet
- Ministerie van Defensie (2021, 4 februari). *Juridische appreciatie activiteiten LIMC.* Den Haag: DJZ. *BS2021002327*
- Ministerie van Justitie en Veiligheid (2018, april). *Big Data verantwoord voorwaarts!.* Den Haag: Directie Informatisering & Inkoop
- NRC Handelsblad, (2020, 16, 17, 23 november, 4 december), diverse artikelen
- Programma aanpak cybercrime (2012, 19 november). *Web Voyager en wet- en regelgeving.* Deelproject wet- en regelgeving
- Volkskrant, (2020, 17, 18 november), diverse artikelen
- Wetenschappelijke Raad voor Regeringsbeleid (2016, 14 april). *WRR-rapportage nr. 95: Big Data in een vrije en veilige samenleving.* Den Haag