Ministerie van Defensie

Onderzoek naar *social media monitoring* bij het ministerie van Defensie

Onderzoek naar naleving gegevensbeschermingswetgeving (Avg/Wpg) bij gebruik *tools* voor monitoring of scraping van *social media*.

Versie	1.0
Datum	25 augustus 2022
Status	Definitief

Colofon

Locatie	Den Haag - Plein-Kalvermarktcomplex Kalvermarkt 32 's-Gravenhage
Postadres	Postbus 20701 2500 ES 'S-GRAVENHAGE MPC 58B
Contactpersoon	Functionaris Gegevensbescherming
Versie	1.0
Opdrachtgever	Functionaris Gegevensbescherming
Auteur	Cluster Gegevensbescherming
Aantal pagina's incl. bijlage(n)	44

Inhoud

1 Inleiding

1.1 Aanleiding onderzoek

Op 7 mei 2021 heeft de minister van Defensie het onderzoeksrapport 'naleving Algemene verordening gegevensbescherming Experimenteeromgeving Land Information Manoeuvre Centre (LIMC)' van de Functionaris Gegevensbescherming (FG) aangeboden aan de Tweede Kamer[1]. Het LIMC was een experimentele eenheid die in een experimentele vorm *Situational Awareness* (SA) en *Situational Understanding* (SU) genereerde voor de CLAS en civiele autoriteiten. LIMC maakte wekelijks een Open Source Intelligence-rapportage (OSINT). OSINT betreft het verzamelen van data en informatie uit open (publiek toegankelijke) bronnen. Om grote hoeveelheden informatie uit open bronnen te kunnen verwerken, werden *tools* ingezet, de zogenaamde *social media monitoring* en *scraping tools.* De eindconclusie van het FG-onderzoek was dat het LIMC niet de intentie had om (grootschalig) persoonsgegevens te verwerken, maar hierin niet volledig is geslaagd. Persoonsgegevens kwamen mee als 'bijvangst'. Tevens werd geconcludeerd dat voor deze verwerking geen wettelijke grondslag bestond en niet was voldaan aan de verantwoordingsplicht waardoor de Algemene verordening gegevensbescherming (Avg) onvoldoende was nageleefd.

Social media is een verzamelnaam voor allerlei internettoepassingen die interactie in zowel tekst als beeld tussen de gebruikers mogelijk maken, zoals *webblogs*, microblogs, fora, foto- en videosites en sociale netwerken. *Social media monitoring tools* worden gebruikt om gegevens over bepaalde sleutelwoorden te verzamelen. Behalve zicht op de berichtenstroom en het aantal berichten, is het bij deze *tools* ook mogelijk om het bereik, het sentiment, de belangrijkste '*influencers*' en veelbesproken onderwerpen te tonen en te analyseren. Dit type *tool* richt zich met name op het inzichtelijk maken van een grote hoeveelheid data en de daaruit voortvloeiende resultaten vervolgens overzichtelijk te presenteren. Daarnaast zijn er *tools*, zoals OSINT-tools[2], gericht op het verzamelen (scrapen) van (persoons)gegevens vanuit publiek toegankelijke bronnen, waaronder *social media*. Door middel van *scraping* kan informatie uit meerdere publiek toegankelijke bronnen gelijktijdig benaderd en doorzocht worden.

Er zijn bij diverse overheidsorganisaties onderzoeken uitgevoerd naar het gebruik van *social media monitoring of –scraping tools* waarbij een aantal zorgpunten rond de naleving van de Avg en de inbreuk op de privacy (persoonlijke levenssfeer) van betrokkenen wordt geuit. Dit betreft bijvoorbeeld een onderzoek naar gemeentelijke online monitoring[3] en een onderzoek van de Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten (CTIVD) over het gebruik van OSINT *tools* door de AIVD en MIVD[4]. Bij de onlinemonitoring activiteiten door NCTV is ook de legitimiteit van het verwerken van persoonsgegevens ter discussie gesteld. De vraagstukken omtrent *social monitoring* spelen zich niet alleen in Nederland af. De Franse toezichthoudende autoriteit, de Commission Nationale d'Information et Libertés (CNIL), heeft bijvoorbeeld voorwaarden gepubliceerd waaronder gegevens

[1] Zie Kamerstuk 2020/21, 32 761, nr 182
[2] Zie ook het Toezichtsrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten. CTIVD nr 24. Vastgesteld op 22 december 2021
[3] Black Box van gemeentelijke online monitoring, Een wankel fundament onder een stevige praktijk. . 2021
[4] CTIVD nr 74 Toezichtsrapport p. 4.

van sociale netwerken in het kader van de verkiezingscampagne mogen worden gebruikt[5].

Het is voor veel instanties onvoldoende duidelijk of wet- en regelgeving ruimte biedt om in het kader van eigen taken en bevoegdheden of ter uitvoering van taken voor andere instanties, persoonsgegevens te verwerken die via het internet verkregen kunnen worden. Na aanleiding van Kamervragen[6] over online monitoring door gemeenten is door het Ministerie van BZK toegezegd een richtlijn/handreiking Monitoring te ontwikkelen waarin aangegeven wordt hoe overheidsorganisaties en uitvoeringsinstanties binnen de kaders van de Avg kunnen monitoren.

In het LIMC-onderzoek was onder andere aanbevolen om de poortwachtersfunctie op het gebied van gegevensverwerking te versterken en om een inventarisatie te doen van risicovolle verwerkingen van persoonsgegevens. De minister van Defensie heeft aangegeven de aanbevelingen van de FG over te nemen[7]. Met dit onderzoek naar het gebruik van applicaties voor het *monitoren* of *scrapen* van *social media* binnen de onderdelen van Defensie[8] geeft de Functionaris voor Gegevensbescherming een eerste aanzet voor de realisatie van deze aanbeveling en vertrekpunt voor totstandkoming en implementatie van toekomstige richtlijnen.

1.2 Doelstelling

De doelstelling van het onderzoek is inzicht geven of Defensie *tools* inzet voor *social media monitoring of scraping activiteiten* en de naleving daarbij van de Avg, Wet politiegegevens (Wpg) en andere gegevensbeschermingsbepalingen[9].

Social media monitoring heeft als gevolg dat persoonsgegevens worden verwerkt en dit brengt een complex juridisch vraagstuk met zich mee. Dit onderzoek dient een bijdrage te leveren aan het verduidelijken van dit juridische vraagstuk en te bepalen of er gehandeld wordt volgens de daarbij geldende regels.

1.2.1 Onderzoeksvragen

De centrale onderzoeksvraag van het onderzoek is:

Maken onderdelen van Defensie gebruik van *tools* voor *social media monitoring of scraping* van publiek toegankelijke bronnen waarbij persoonsgegevens[10] verwerkt worden? En zo ja, worden daarbij de Avg, Wpg en andere gegevensbeschermingsbepalingen nageleefd?

---

[5] Communication politique : quelles règles pour la collecte de données sur les réseaux sociaux ? | CNIL

[6] Zie TK 2020-2021, nr. 3431 Aanhangsel van de Handelingen. Antwoorden d.d. 2 juli 2021 op schriftelijke vragen van het lid Leijten (SP) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat gemeenten mensen online in de gaten houden ingezonden 25 mei 2021

[7] Zie TK 2020-2021, 32761 nr.182 Verwerking en bescherming persoonsgegevens, Brief van de Minister van Defensie (aanbieding onderzoeksrapport over experimentele LIMC d.d. 7 mei 2021, pagina 5/6 *Deze aanbeveling beoogt het risicobewustzijn bij de (mogelijke) verwerking van persoonsgegevens bij behoeftestellers en inkopers te verhogen… De komende tijd gaat een extern bureau nader onderzoek doen naar de naleving van de AVG bij de informatieactiviteiten van de verschillende defensieonderdelen….*

[8] Met uitzondering van de MIVD.

[9] Uitvoeringswet Algemene verordening gegevensbescherming, Regeling AVG Defensie, Regeling Wpg Defensie, Regeling Gegevensbescherming Militaire Operaties (RGMO).

[10] In de Avg en de Wpg is een persoonsgegeven gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Zie onder A.1.2 voor een nadere toelichting.

Deelvragen:

1. Heeft Defensie *social monitoring of scraping tools* aangekocht en/of in gebruik?
2. Worden bij het gebruik van deze *tools* persoonsgegevens verwerkt en met welk doel wordt dit gedaan?
3. Is bij de inkoop voldaan aan de Avg of Wpg en is indien van toepassing het gebruik van een *tool* of applicatie overeenkomstig het onderliggende contract met de verwerker?
4. Op welke grondslag is het gebruik gebaseerd? Binnen welke taak van het betreffende organisatieonderdeel valt het proces/verwerking?
5. In hoeverre zijn verwerkingen waarbij gebruik wordt gemaakt van dergelijke *tools* in overeenstemming met de Avg en Wpg ingericht en gedocumenteerd?

1.3 Reikwijdte

Dit onderzoek richt zich op alle onderdelen van Defensie met uitzondering van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD)[11].

Dit onderzoek heeft betrekking op zowel de bedrijfsvoerings- en ondersteunende processen als op de operationele processen van Defensie. Onderzocht zijn: Bestuursstaf (BS), Directie Operaties (DOPS), Koninklijke Marechaussee (KMAR), Commando Zeestrijdkrachten (CZSK), Commando Luchtstrijdkrachten (CLSK), Commando Landstrijdkrachten (CLAS), Defensie Ondersteuningscommando (DOSCO), Defensie Materieel Organisatie (DMO) en Joint Informatievoorziening Commando (JIVC).

Het onderzoek betreft zowel het naleven van de Avg als van de Wpg.

1.4 Leeswijzer

Dit rapport is als volgt opgebouwd: na het inleidende hoofdstuk volgt een samenvatting met aanbevelingen voor de inzet van *tools* voor het *monitoren of scrapen* van onder andere *social media*. Het derde hoofdstuk gaat in op het gebruik van *tools* voor onder andere *social media monitoring* en het verwerken van persoonsgegevens. In hoofdstuk vier wordt de onderzoekmethode en werkzaamheden kort toegelicht.

In bijlage A is het van toepassing zijnde juridische kader opgenomen. In bijlage B is een checklist opgenomen die gebruikt kan worden bij de afweging of het verzamelen, analyseren of anderszins verwerken van (persoons)gegevens van publiek toegankelijke bronnen waaronder *social media* toegepast mag worden. In bijlage C is een overzicht van afkortingen en begrippen opgenomen.

Daar waar nodig zijn specifieke bevindingen gedeeld met het betreffende onderdeel van Defensie, opdat verbetermaatregelen kunnen worden genomen.

[11] De werkzaamheden van de MIVD hebben een basis in de Wet op de inlichtingen- en veiligheidsdiensten 2017

2 Hoofdboodschap: conclusies en aanbevelingen

In de eindrapportage van het LIMC-onderzoek was door de FG onder andere aanbevolen om de poortwachtersfunctie op het gebied van gegevensverwerking te versterken en een inventarisatie te doen van risicovolle verwerkingen van persoonsgegevens. Met dit vervolgonderzoek naar het gebruik van *tools* binnen de onderdelen van Defensie[12] die ingezet worden voor *social media monitoring* of anderszins verzamelen en analyseren van (persoons)gegevens van publiek toegankelijke bronnen geeft de FG een aanzet voor de realisatie van deze aanbevelingen. De doelstelling van dit onderzoek is inzicht te geven of Defensie *tools* inzet voor *social media monitoring* of *-scraping* activiteiten en de naleving daarbij van de Avg, Wpg en andere gegevensbeschermingsbepalingen[13].

De informatie-omgeving is volop in ontwikkeling met grote gevolgen voor de omgeving waarin de krijgsmacht opereert en voor het opereren van de krijgsmacht zelf. Diverse voorbeelden van buitenlandse bedreigingen[14] voor de vrijheid in Nederland en het Koninkrijk halen de media. Deze dreigingen spelen zich steeds vaker af in het digitale domein, bijvoorbeeld in de vorm van cyberaanvallen, beïnvloeding en informatie gedreven inzet van de krijgsmacht van vreemde mogendheden[15]. De Defensievisie-2035 stelt dat een van de drie eigenschappen van de krijgsmacht is dat deze naast technologisch hoogwaardig en een betrouwbare partner en beschermer, ook informatiegestuurd moet zijn. Het gaat hierbij om moderne IT die nodig is om voor de hoofdtaken van Defensie grote hoeveelheden informatie te verzamelen en snel te verwerken, onder andere zodat de commandant tijdig betrouwbare informatie ontvangt. Dit is cruciaal voor de werkzaamheden van Defensie, voor de bescherming van de eigen mensen en voor de bescherming van de bevolking in de omgeving waarin de krijgsmacht opereert. Expertise kan alleen worden opgebouwd en in stand gehouden worden als medewerkers mogen en kunnen trainen, net zoals militairen trainen met bijvoorbeeld vuurwapens. Het is echter niet vanzelfsprekend om te oefenen in het informatiedomein omdat dit kan leiden tot een inbreuk op de persoonlijke levenssfeer[16] van betrokkenen en het verwerken van persoonsgegevens van betrokkenen. De noodzaak die de onderdelen van Defensie voelen om nieuwe werkwijzen en technologische middelen toe te passen om hun taak effectief uit te kunnen voeren in de informatie-omgeving wringt met de bestaande wettelijk kaders van de taken en bevoegdheden.

De technologische ontwikkelingen en de groei in het gebruik van *social media* van de afgelopen jaren hebben geleid tot een sterke groei in het aantal beschikbare *tools* met een scala aan technologische mogelijkheden voor het doorzoeken, verzamelen en met elkaar in verband brengen van een grote hoeveelheid data. Er zijn ook bedrijven die gespecialiseerde datasets aanbieden die door deze bedrijven zelf zijn geaggregeerd op basis van onder andere gegevens gescrapet van publiek toegankelijke bronnen. De ontwikkeling van digitalisering gaat in een hoog tempo; wet- en regelgeving en beleidsvorming kunnen niet altijd met dit tempo meebewegen.[17] Tegelijk heeft de overheid een zware verantwoordelijkheid om steeds rechtsstatelijkheid, democratische verantwoording en publieke belangen als

[12] Met uitzondering van de MIVD.
[13] Uitvoeringswet Algemene verordening gegevensbescherming, Regeling AVG Defensie, Regeling Wpg Defensie, Regeling Gegevensbescherming Militaire Operaties.
[14] Kamerbrief antwoorden aan op de feitelijke vragen over de 'Hoofdlijnen beleid Ministerie van Defensie', ingezonden op 25 februari 2022, vraag 38.
[15] Defensievisie 2035: Vechten voor een veilige toekomst p.8.
[16] Art 8 van het Europees Verdrag voor de Rechten van de Mens: Een ieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Zie 3.2 en 3.3. voor nadere informatie.
[17] Rijksinspecties. Programma Innovatie Toezicht. Nieuwe technologieën en nieuwe samenwerkingen.

privacy te borgen en te bewaken en moet deze zich dus bewust zijn van ethiek en risico's als gevolg van inzet van nieuwe technologische middelen en gebruik van data.

Defensie heeft, evenals andere overheidsorganisaties, beperkt beleid en richtlijnen voor het gebruik van *tools* ten behoeve van verzamelen en analyseren van (persoons)gegevens van publiek toegankelijke bronnen. Ook bij diverse andere overheidsorganisaties zijn recent onderzoeken uitgevoerd naar het gebruik van *social media monitoring* of *–scraping tools* waarbij vergelijkbare aandachtspunten worden geconstateerd. Dit betreft bijvoorbeeld het onderzoek naar online monitoring door gemeenten[18], naar aanleiding waarvan door het Ministerie van BZK is toegezegd een richtlijn/handreiking Monitoring[19] te ontwikkelen waarin aangegeven wordt hoe overheidsorganisaties en uitvoeringsinstanties binnen de kaders van de Avg kunnen monitoren. In het CTIVD onderzoeksrapport[20], over het gebruik van OSINT-tools door de AIVD en MIVD, wordt aanbevolen om voldoende waarborgen te creëren ten aanzien van *social monitoring* en een gezamenlijk beleidskader te ontwikkelen met bijbehorende werkinstructies.

2.1 Conclusies

Het uitgevoerde onderzoek leidt tot de volgende conclusies en aanbevelingen.

1. Uit een eerste inventarisatie blijkt dat bij Defensie diverse *social media monitoring* en *scraping* tools worden of zijn ingezet. Er wordt of werd gebruikgemaakt van onder andere producten en diensten van *Webint, Coosto, Meltwater, OBI4WAN, Tweetdeck, Lexis Nexis, Public Sonar, KALI Linux, Twint, 2meter1 analytics&online marketing.* Het gebruik van meerdere tools is inmiddels door Defensie stopgezet in afwachting van nadere richtlijnen en totdat aan de wettelijke verantwoordingsplicht en waarborgen is voldaan.

2. Bij het gebruik van deze tools worden persoonsgegevens verwerkt.
   Uit de inventarisatie blijkt dat de *tools* worden of zijn ingezet voor diverse doeleinden in de operationele taakuitvoering, de politietaak, de bedrijfsvoerings- en ondersteunde processen. Bijvoorbeeld voor het onderkennen en onderzoeken van cyberbedreigingen, militaire tactische inzichten, werving & selectie en communicatie. Een deel van de *tools* is bijvoorbeeld gebruikt ten behoeve van operationele processen om informatie te verzamelen en te analyseren uit publiek toegankelijke bronnen, waaronder nieuws- en *social media sites,* zonder specifiek gericht te zijn op het verzamelen van persoonsgegevens. Te denken valt aan het bevorderen van *situational awareness* van de commandant in het kader van de inzet van militairen. Daarnaast zijn *tools* in gebruik bij bedrijfsvoering en ondersteunende processen bijvoorbeeld voor communicatie doeleinden zoals *webcare*, sentimentanalyses en het volgen van actuele berichtgeving en het sociaal maatschappelijke discours ten aanzien van Defensie gerelateerde onderwerpen. Ook worden *tools* ingezet bij openbronnenonderzoek voor de KMar-politietaak bij de strafrechtelijke handhaving van de rechtsorde en handhaving van de openbare orde.

   Vanwege de brede wettelijke definities van wat *persoonsgegevens zijn* en van wat onder een *verwerking van persoonsgegevens moet worden verstaan*, volgt dat bij het gebruiken van *social monitoring* en *scraping tools* er onvermijdelijk sprake is van verwerkingen van persoonsgegevens of politiegegevens. Wanneer

[18] Black Box van gemeentelijke online monitoring, Een wankel fundament onder een stevige praktijk. [redacted]. 2021
[19] Zie TK 2020-2021, nr. 3431 Aanhangsel van de Handelingen. Antwoorden d.d. 2 juli 2021 op schriftelijke vragen van het lid Leijten (SP) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat gemeenten mensen online in de gaten houden ingezonden 25 mei 2021
[20] CTIVD nr. 74 Toezichtsrapport p. 4.

tijdens of voorafgaand aan het analyse- en productieproces verwijdering, pseudonimisering of anonimisering van persoonsgegevens plaatsvindt, zijn dit immers ook al verwerkingen van persoonsgegevens.

3. Uit de inventarisatie wordt onvoldoende inzichtelijk of bij inkoop of ingebruikname van de *tools* er toereikende aandacht was voor de potentiële inbreuk die een *tool* zou kunnen hebben op fundamentele rechten (recht op privacy) van de betrokkenen en de afweging en beoordeling van de proportionaliteit en subsidiariteit van het middel.

   Dit wordt waarschijnlijk veroorzaakt doordat bij medewerkers niet duidelijk was dat bij gebruik van *social monitoring of -scraping tools* persoonsgegevens worden verwerkt en dat daarom voor het verwerken een wettelijke grondslag nodig is. Doordat *tools* ook gratis verkrijgbaar en *webbased* zijn, verloopt de verwerving en ingebruikname niet via de reguliere inkoopprocessen. De beoogde poortwachtersfunctie van inkopers en behoeftesteller is mede daardoor niet gewaarborgd.

   Een belangrijke verbetering is dat het bewustzijn zichtbaar is verhoogd. De FG ziet dat sinds het onderzoek naar LIMC en de aandacht die dat onderzoek heeft gekregen er meer bewustwording is voor de juiste omgang met persoonsgegevens en de daarbij behorende kaders. De voor dit onderzoek uitgevoerde inventarisatie naar het gebruik van *social monitoring* en *scraping tools* heeft dit effect binnen Defensie verder versterkt.

4. Bij meerdere verwerkingen is verbetering nodig voor wat betreft de rechtmatige uitvoering van taken en bevoegdheden en de naleving van de Avg, de Wpg en de Regeling Gegevensbescherming Militaire Operaties (RGMO). De geconstateerde tekortkomingen brengen risico's met zich mee voor onder andere de rechtmatige uitvoering (het hebben van een rechtmatig doel en wettelijke grondslag) voor de betreffende verwerkingen.

   Het gebruik van meerdere tools, voornamelijk in gebruik voor de operationele taakuitvoering, waarbij deze tekortkomingen zijn geconstateerd, zijn inmiddels door Defensie stopgezet in afwachting van nadere richtlijnen. De nog in gebruik zijnde tools worden voornamelijk gebruikt voor communicatie, werving & selectie, beveiliging van de IT-infrastructuur en locaties en uitvoering van de politietaak.

   De huidige juridische kaders geven beperkte mogelijkheden[21] voor het gebruik van *tools* voor het verwerken van persoonsgegevens van publiek toegankelijke bronnen waaronder *social media sites* voor de taken van Defensie. Vooral voor de mogelijkheden om te oefenen en om voor te bereiden op inzet geeft dit knelpunten. Om deze beperkingen en knelpunten op te lossen zal onderzocht moeten worden of dit binnen de bestaande taakstelling en bevoegdheden van Defensie mogelijk is. Daarna kan bezien worden of aanvullende bevoegdheden nodig zijn. Hierbij moet ook gekeken worden naar welke verschillende rollen en taken reeds zijn toebedeeld aan defensie- en overheidsdiensten zoals de KMar, Politie en MIVD.

   Voor de taken die de KMar uitvoert, die hun wettelijke grondslag in de Politiewet 2012 vinden, zijn de mogelijkheden ruimer en zijn aanvullende richtlijnen beschikbaar voor het juist en rechtmatig toepassen van openbronnenonderzoek.

[21] Nota Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatieomgeving. Ministerie van Defensie / Directie Juridische Zaken. 12 april 2021. Zie ook paragraaf 3.4.2 en bijlage A.

Overheidsinstanties kunnen zich bij verwerkingen in het kader van het uitoefenen van *hun taken* niet beroepen op de grondslag van gerechtvaardigd belang. Voor een beroep op deze grondslag is echter wel beperkt ruimte bij typische bedrijfsmatige handelingen. Er zijn over het gebruik van gerechtvaardigd belang als rechtmatige grondslag door overheden en de belangenafweging die benodigd is, weinig richtlijnen en/of jurisprudentie beschikbaar. Daardoor is het niet mogelijk om een volledig overzicht te geven van de soort verwerkingen waarop een dergelijke grondslag van toepassing kan zijn. Dit zal per verwerking afgewogen moeten worden. Hierbij dient altijd een transparante afweging te worden gemaakt of de verwerking van persoonsgegevens noodzakelijk is voor de behartiging van het gerechtvaardigd belang en of de belangen en de fundamentele vrijheden van de betrokkenen niet zwaarder wegen.[22]

Nadere kaders zijn nodig voor een juiste en eenduidige interpretatie en toepassing van de rechtmatige verwerkingsgrondslag. Dit gaat Rijksbreed en binnen Defensie om zeer uiteenlopende processen en taken en daarbij toepasselijke bevoegdheden, voorwaarden en beperkingen.

5. Het naleven van de privacywetgeving bij Defensie behoeft verbetering. Dit betreft bijvoorbeeld het gebrekkig naleven van de verantwoordingsplicht waaronder het uitvoeren van *Data Protection Impact Assessments* (DPIA's). Daarnaast zijn niet alle benodigde verwerkersovereenkomsten en analyse van de toepasselijke gebruikersvoorwaarden aangetroffen. Hierdoor is het niet volledig inzichtelijk welke afspraken gelden met verwerkers en of de toepasselijke gebruikersvoorwaarden zijn beoordeeld en in de praktijk worden nageleefd. Tevens is meer aandacht nodig voor het inzichtelijk uitvoeren en motiveren van een belangenafweging en het inrichten van afdoende waarborgen om disproportionele inbreuken op de persoonlijke levenssfeer te voorkomen. Voor betrokkenen kan het, door gebrekkige transparantie, onvoldoende duidelijk zijn of, waarom en welke persoonsgegevens worden verwerkt.

   Ook hier ziet de FG dat sinds het onderzoek naar LIMC er maatregelen ter verbetering worden getroffen. Bijvoorbeeld wordt voor de *monitoring* van *(social) media* door de directie Communicatie een DPIA opgesteld en de verwerkersovereenkomst opgelopen. Voor het gebruik van *social monitoring* door werving en selectie en voor de bescherming van de IT-infrastructuur van Defensie zijn recentelijk DPIA's vastgesteld.

De onderzoekers geven aanbevelingen aansluitend op deze samenvatting en een handelingsperspectief in de vorm van een checklist voor de benodigde afweging (zie bijlage B).

[22] Zie artikel 6 lid 1f Avg: *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.*

2.2 Aanbevelingen

De aanbevelingen op grond van de bevindingen en conclusies zijn:

1. *Zorg voor aanvullend beleid, richtlijnen en werkinstructies*
   Draag zorg voor voldoende waarborgen ten aanzien van een rechtmatig gebruik van *social media monitoring* en -*scraping tools*, de toegestane activiteiten en te monitoren- of te scrapen bronnen. Het vraagstuk rondom het toepassen van *social monitoring* door overheidsinstanties is complex en er is weinig jurisprudentie en slechts zeer beperkt toepasselijke *guidelines* vanuit de Autoriteit Persoonsgegevens (AP) en de European Data Protection Board (EDPB) beschikbaar. Mede naar aanleiding van het rapport 'Blackbox online monitoring bij gemeenten onderzocht' laten de Minister van BZK en de Minister voor Rechtsbescherming onderzoek uitvoeren naar de knelpunten en oorzaken voor tekortkomingen in de naleving van de Avg door overheden. Dit onderzoek wordt uitgevoerd door het WODC[23].
   Zolang de door het ministerie van BZK toegezegde richtlijn/handreiking nog niet gereed is[24], moet Defensie zelf zorgen voor toereikende kaders en richtlijnen om verantwoordelijk en rechtmatig gebruik te maken van *social media monitoring* en -*scraping* tools.

2. *Hanteer willen, mogen en kunnen in de juiste volgorde*
   Zorg dat voor het toepassen van social monitoring of -scraping binnen verwerkingen het doel en de grondslag duidelijk zijn en leef de rechtswaarborgen en de verantwoordingsplicht[25] na.
   Indien de behoefte om *social media monitoring of –scraping* te gebruiken om legitieme doeleinden te bereiken groter is dan de huidige juridische kaders toelaten, bijvoorbeeld door ontwikkelingen in het informatiedomein, zal eerst onderzocht moeten worden of dit binnen de bestaande taakstelling en bevoegdheden van Defensie mogelijk is. Daarna kan bezien worden of aanvullende bevoegdheden nodig zijn. Hierbij moet ook gekeken worden naar welke verschillende rollen en taken reeds zijn toebedeeld aan defensie- en overheidsdiensten zoals de KMar, Politie en MIVD.

3. *Zorg bij het verwerven of ingebruikname van (gratis) tools voor een transparante afweging van het verantwoord gebruik ervan*
   Ter beoordeling van de rechtmatigheid en proportionaliteit van de verwerking is van belang dat voorafgaand aan het gebruik duidelijk is voor welk doel het wordt ingezet en dat bekend is hoe de *tool* werkt. Bijvoorbeeld welke bronnen worden geraadpleegd, welke gegevens worden opgeslagen, tot welke gegevens (waaronder gebruiksgegevens) de leverancier toegang heeft en wat met de gegevens gebeurt als de samenwerking stopt.
   Indien van toepassing dienen de verwerkersovereenkomsten of –afspraken te worden vastgesteld en dient een beoordeling van de gebruikersovereenkomst en –voorwaarden plaats te vinden. Tevens is van belang dat de mate van inbreuk op de persoonlijke levenssfeer, het belang van ethisch verantwoord handelen en de gevoeligheid van de informatie in de afweging wordt meegenomen. Hiertoe wordt ook aanbevolen de diversiteit aan *tools* die binnen Defensie gebruikt mogen worden, waar mogelijk, te beperken.

---

[23] Zie Wetenschappelijk Onderzoeks- en Documentatiecentrum Projectnummer 3301
[24] Zie TK 2020-2021, nr. 3431 Aanhangsel van de Handelingen. Antwoorden d.d. 2 juli 2021 op schriftelijke vragen van het lid Leijten (SP) aan de Minister van Binnenlandse Zaken en Koninkrijksrelaties over het bericht dat gemeenten mensen online in de gaten houden ingezonden 25 mei 2021.
[25] Zie artikel 5 lid 2 Avg.

4. *Investeer in de Avg-coördinatiefunctie en Wpg-privacyfunctionaris*
   Verwezen wordt naar de aanbeveling in het FG Toezichtjaarverslag 2021 om de Avg-coördinatiefunctie te versterken en te professionaliseren en de samenwerking met de juridische en operationele lijn te intensiveren. Investeer in het vergroten van capaciteit en kennisniveau, zowel kwantitatief en kwalitatief, waar noodzakelijk.

2.3 Handelingsperspectief / Checklist

Er is geen '*one size fits all'* handreiking te geven voor wanneer het toepassen van *social media monitoring of –scraping* activiteiten binnen Defensie legitiem is. Bij elk doel waarbij inzet van *tools* noodzakelijk wordt geacht zal moeten worden vastgesteld of er een grondslag is voor de verwerking van persoonsgegevens.

Bij inzet van een tool moet de noodzaak van het gebruik ten opzichte van de proportionaliteit en subsidiariteit van deze inbreuk aantoonbaar worden afgewogen en moeten de benodigde maatregelen ter beperking van inbreuk worden bepaald. Zo moet worden gekeken naar het doel van een inbreuk. Dit doel moet kunnen worden aangemerkt als "legitiem" in een democratische samenleving. Wanneer sprake is van een legitiem doel, dient vervolgens te worden gekeken naar de (maatschappelijke) noodzaak van de voorgenomen inbreuk in verhouding tot dit legitieme doel. Hierbij speelt een rol of de voorgestelde inbreuk geschikt is om dat doel te bereiken en daarbij niet verder wordt gegaan dan noodzakelijk is (proportionaliteit), of minder ingrijpende middelen voorhanden zijn om hetzelfde resultaat te bereiken (subsidiariteit) en of afdoende waarborgen zijn ingesteld om disproportionele inbreuken en willekeur te voorkomen. Hoe groter de inbreuk op de privacy des te meer maatregelen genomen moeten (kunnen) worden om de risico's te beperken.

Per geval is maatwerk nodig om de rechtmatigheid en behoorlijkheid af te wegen, waarbij aandacht is voor de reikwijdte van de verwerking en de benodigde maatregelen om de risico's te beperken te bepalen. In afwachting van nadere kaders[26] wordt aanbevolen om voor de afweging of een tool toegepast mag worden per verwerking (gebruik van een *too*l) minimaal aantoonbaar de stappen te doorlopen zoals opgenomen in de checklist in Bijlage B.

[26] Kamervragen 2020-2021, nr. 3431.

3 Bevindingen *social media monitoring* en naleving van de Avg en Wpg

3.1 Social media monitoring of -scraping

3.1.1 Toelichting begrippen

Social media is een verzamelnaam voor allerlei internettoepassingen die interactie in zowel tekst als beeld tussen de gebruikers mogelijk maken, zoals *webblogs*, microblogs (zoals Twitter), fora, videosites en sociale netwerken (zoals Facebook).

Social media monitoring is het bijhouden en analyseren van uitingen in de sociale media. Dit kan voor verschillende doeleinden worden toegepast zoals het snel op vragen en kritiek vanuit de samenleving/consumenten kunnen reageren, het analyseren van trends (bijv. of men positief of negatief spreekt over een organisatie), voor het monitoren van evenementen ten behoeve van de veiligheid en beveiliging of *situational awareness*.

Bij *tools* gaat het om *software* met bijvoorbeeld zoek- en netwerkanalysefuncties, waarbij een groot aantal (publiek toegankelijke) bronnen gelijktijdig kan worden bevraagd zoals *social media*, *video sharing site*s, wiki's, blogs, *darknet*, *document sharing platforms*, *whois data,* kranten en openbaar gemaakte bestanden afkomstig uit data-lekken. Dit kunnen zogenaamde *social media monitoring tools* zijn, zoals *webbased* applicaties, die gericht (persoons)gegevens verzamelen van *social media* op basis van bepaalde *keywords*, zoals een bepaalde bedrijfstak, een dienst, een incident, een persoon of een evenement. Het kunnen ook *tools zijn*, zoals *OSINT-tools*[27], gericht op het verzamelen (scrapen) van (persoons)gegevens van publiek toegankelijke bronnen, waaronder *social media*. De *tools* kunnen allerlei websites en sociale netwerken zoals fora, blogs, nieuwssites, *social media* diensten zoals *Facebook, Twitter, Instagram en YouTube* doorzoeken.

In toenemende mate zijn er commerciële partijen die *tools* beschikbaar stellen en diverse bronnen toegankelijk maken. Deze *tools* maken het eenvoudig om relevante gegevens snel en gelijktijdig uit veel verschillende toegankelijke bronnen te verzamelen, te monitoren, te analyseren enzovoort. De manier waarop de *tools* werken en de reikwijdte verschillen wel van elkaar.[28] Er zijn ook *tools* zoals *search engines* die niet per definitie gericht zijn om op informatie verzamelen van *social media* maar in de zoekresultaten toch gegevens die afkomstig zijn vanuit *social media* weergeven. Er zijn ook commerciële partijen die gespecialiseerde datasets die door henzelf zijn geaggregeerd aanbieden.[29] De datasets kunnen onder meer bestaan uit *scraped* data uit *social media* bronnen of gelekte datasets die online gepubliceerd zijn. Deze *tools* zorgen voor hogere efficiëntie maar de privacy-inbreuk voor de betrokkenen kan ingrijpender zijn. Wanneer het niet duidelijk is waar die gegevens vandaan komen en of ze rechtmatig zijn verzameld mogen ze niet gebruikt worden.

---

[27] Zie ook het Toezichtsrapport Automated OSINT: *tools* en bronnen voor openbronnenonderzoek van de Commissie van toezicht op de inlichtingen- en veiligheidsdiensten. CTIVD nr. 24. Vastgesteld op 22 december 2021

[28] In het rapport van CTIVD over *automated*-OSINT is een nadere toelichting opgenomen over de wijze waarop *tools* raadplegen via webbrowser of app, met gebruik van een Application Programming Interface (API) en gespecialiseerde *tools* werken.

[29] Toezichtsrapport Automated OSINT: *tools* en bronnen voor openbronnenonderzoek. CTIVD

3.1.2 *Verwerken persoonsgegevens bij gebruik tools*

Bij een deel van de *tools* worden door middel van zelf opgestelde *query's*[30] gerichte zoekslagen door beschikbare *social media bronnen* gedaan. *Social media posts* die aan de query voldoen worden door de *tool* verzameld en gepresenteerd op een dashboard. Aangegeven is dat niet specifiek gezocht wordt op persoonsgegevens – de gebruikte termen zijn generiek – maar de betreffende berichten/posts kunnen persoonsgegevens bevatten of kunnen herleidbaar zijn tot identificeerbare personen. Bijvoorbeeld doordat de hele tweet of post weergegeven wordt in een dashboard of doordat een link is opgenomen naar een relevante post. Uit informatie van een verwerker blijkt dat van personen wiens gegevens openbaar toegankelijk zijn, de (profiel)namen, (profiel)foto's, openbare accountinformatie, locatiegegevens en eventuele andere persoonlijke informatie in de inhoud van berichten verwerkt worden. Dit laatste kan ook bijzondere of gevoelige persoonsgegevens bevatten zoals politieke overtuigingen.
Daarnaast zijn er *tools* die (persoons)gegevens uit publiek toegankelijke bronnen verzamelen, waaronder nieuws- en *social media* websites. De verzamelde gegevens worden geanalyseerd en verwerkt in rapportages bijvoorbeeld ten behoeve van *situational awareness*, waarbij persoonsgegevens zoveel als mogelijk worden verwijderd, gepseudonimiseerd of geanonimiseerd. Hoewel niet gericht wordt gezocht op personen, worden bij het uitvoeren van *social media monitoring* of –*scraping* opdrachten persoonsgegevens door de *tools* verwerkt en kunnen persoonsgegevens verwerkt zijn in de eindproducten.

Aangegeven is dat bij gebruik van de *tools* maatregelen kunnen worden toegepast om de (onbedoeld) verzamelde persoonsgegevens te pseudonimiseren of te anonimiseren. Uit de ontvangen informatie is echter niet af te leiden of de maatregelen voldoende ingericht kunnen worden om uit te sluiten dat de verzamelde gegevens niet meer herleidbaar zijn naar een identificeerbaar natuurlijk persoon. Daarbij geldt dat ook met het toepassen van maatregelen er in het kader van artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) sprake is van een inbreuk op iemands recht op eerbiediging van privé-, familie- en gezinsleven plaatsvindt wanneer dergelijks *tools* gebruikt worden om *social media* te doorzoeken. Er dient dus altijd een afweging plaats te vinden of het gebruik rechtmatig, behoorlijk en transparant is en geen onrechtmatige of onevenredige inmenging in de persoonlijke levenssfeer van de betrokkene oplevert.

Bij gebruik van *tools* die gebruikt worden voor de uitvoering van de politietaak wordt doorgaans wel gericht gezocht met gebruik van persoonsgegevens om (persoons)gegevens te verkrijgen. Dit dient plaats te vinden op basis van de geldende wet- en regelgeving (Politiewet, Wpg en Wetboek van Strafvordering).

Het maakt ook geen verschil dat een verwerkingsverantwoordelijke een gegeven niet zal gebruiken om een persoon mee te identificeren. Het feit dat de mogelijkheid bestaat bij de verwerkingsverantwoordelijke of bij een derde om dit te doen, is voldoende[31].

3.1.3 *Gebruik van tools bij Defensie*

Ten behoeve van dit onderzoek is via de Avg-coördinatoren en de Wpg-privacyfunctionaris aan de onderdelen van Defensie gevraagd een inventarisatie te maken van binnen hun defensieonderdeel in gebruik zijnde *tools* voor *social media monitoring of –scraping*. De inventarisatie betrof alle mogelijke vormen van *social media monitoring* met gebruik van *tools* onafhankelijk van de taak en het doel waarvoor deze worden toegepast. Uit een eerste inventarisatie blijkt dat binnen Defensie meerdere *tools* worden of zijn gebruikt voor uiteenlopende taken en

[30] Bijvoorbeeld de zoekterm 'defensie', waarbij ook een aantal termen worden aangeven die uitgesloten moeten worden van de zoekslag om irrelevante gegevensverzameling te voorkomen.
[31] Zie bijv. *HvJ EU* 19 oktober 2016, ECLI:EU:C:2016:779.

doeleinden. Dit betreffen bijvoorbeeld aangeschafte licenties, gratis webbased *tools* of *tools* die door Defensie zelf worden ontwikkeld. Uit de inventarisatie blijkt dat er gebruik wordt of werd gemaakt van onder andere producten en diensten van *Webint, Coosto, Meltwater, OBI4WAN, Tweetdeck, Lexis Nexis, Public Sonar, KALI Linux, Twint, 2meter1 analytics&online marketing.* Het gebruik van meerdere *tools* is inmiddels door Defensie stopgezet in afwachting van nadere richtlijnen en totdat aan de wettelijke verantwoordingsplicht en waarborgen is voldaan zoals het opstellen van DPIA's. Dit betreft voornamelijk het gebruik van *tools* ten behoeve van operationele taken. De nu nog in gebruik zijnde *tools* worden voornamelijk gebruikt voor communicatie, werving en selectie, beveiliging van de IT-infrastructuur, beveiliging van locaties en uitvoering van de politietaak.

Van een aantal *tools*, zoals *Polpo, Brandwatch* en *Everstream*, werd tijdens het opstellen van het rapport nog afgewogen of ze in gebruik zullen worden genomen, *Analytics*. Daarnaast is Defensie is bezig met innovatietrajecten waarbij mogelijk *social media monitoring* of *-scraping* activiteiten een rol kunnen gaan spelen.

3.1.4 Doelen inzet tools

Binnen Defensie worden of zijn *tools* ingezet voor:

- KMar-politietaken bij de strafrechtelijke handhaving van de rechtsorde en handhaving van de openbare orde.
- Informatiegestuurd optreden, het monitoren van gebeurtenissen en crisissituaties voor het krijgen van situational awareness en om voorspellingen te kunnen doen over wat er mogelijk nog gaat komen.
- Ondersteuning van v*ulnerability management*, *cyber threat intelligence* en *cyber security intelligence* met actuele informatie met als doel bijvoorbeeld de bescherming van de IT-infrastructuur.
- Webcare soms in combinatie met monitoring. Via *social media* kan inzicht worden verkregen in wat er speelt binnen doelgroep(en) en kan in de gaten wordt gehouden wat voor soort vragen of klachten er zijn om hierop in te kunnen spelen.
- Het krijgen van inzicht in de sociaal-maatschappelijk en politiek-bestuurlijke omgeving rond Defensie en het volgen van actuele berichtgeving en het sociaal maatschappelijke discours ten aanzien van Defensie gerelateerde onderwerpen.
- Het monitoren van trends of opstellen van sentimentanalyses. Hiermee kan bijvoorbeeld inzicht verkregen worden in wat voor soort persberichten, evenementen of initiatieven veel of juist minder reactie opwekken.

3.2 Afweging bij gebruik *tools*

In bijlage A is een overzicht opgenomen van het van toepassing zijnde juridische kader.

3.2.1 *"Openbare gegevens"*

Het is een onjuiste aanname dat informatie uit publiek toegankelijk (openbare) bronnen[32] vanwege dat openbare karakter zonder beperking mag worden gebruikt. De term 'open bron' of 'publiek toegankelijke bron' suggereert dat iedereen vrij is om de data naar eigen wens en inzicht te gebruiken. Dat is echter niet het geval.[33] Het "openbare" of "vrij toegankelijke" karakter van de gegevens die beschikbaar zijn op sociale netwerken maakt niet dat ze de status van persoonsgegevens verliezen en de betrokkenen om wiens gegevens het gaat geen recht op eerbiediging van hun persoonlijke levenssfeer meer hebben.

De intentie van de betrokkene, het 'data subject', moet worden meegewogen. Alleen als de betrokkene zelf de intentie had om informatie openbaar te maken, dan is het openbaar. Het feit dat derden informatie over een betrokkene publiek gemaakt hebben, maakt deze informatie voor de privacy-afweging nog niet openbaar. Tenzij op basis van objectieve feiten en omstandigheden kan worden vastgesteld dat het niet anders kan dan dat de betrokkene *zelf* informatie openbaar heeft willen maken, is het niet openbaar en valt het onder de bescherming van artikel 8 van het EVRM en artikel 10 van de Grondwet[34]. Artikel 8 van het EVRM beschrijft het recht op eerbiediging van privé-, familie- en gezinsleven. Artikel 10 van de grondwet geeft aan dat een inbreuk op inmenging op het recht op eerbieding van de persoonlijke levenssfeer gerechtvaardigd kan zijn mits die beperking een grondslag vindt 'bij of krachtens' de wet.

Gegevens die op *social media sites* worden gezet door burgers, worden gepubliceerd met een bepaald doel en mogen niet zondermeer voor een ander doel worden gebruikt. Persoonsgegevens die openbaar beschikbaar (publiek toegankelijke bronnen) zijn kunnen niet voor nieuwe/andere doeleinden worden verwerkt zonder een geldige wettelijke grondslag[35]. Het feit dat het gaat om gegevens uit openbare bronnen doet niet af dat aan de verplichtingen[36] die voortkomen uit de Avg of Wpg, alsmede dat het gebruik in overeenstemming moet zijn met artikel 8 EVRM en artikel 10 Grondwet. Er dient bij de afweging ook rekening te worden gehouden met de redelijke verwachtingen van de betrokkenen in de context waarin de gegevens zijn verzameld zoals een eventuele koppeling tussen die doeleinden en de doeleinden van de voorgenomen verdere verwerking.

Er dient ook aandacht te zijn voor de oorsprong van de verzamelde gegevens. Indien een tool bijvoorbeeld gegevens haalt uit websites waarvan de algemene gebruiksvoorwaarden het hergebruik van gegevens beperken is het onwaarschijnlijk

---

[32] "Open bronnen kenmerken zich doordat in beginsel eenieder er toegang toe kan verkrijgen en dat voor zover toegang gebonden is aan een account, het verkrijgen van een account een (semi-)geautomatiseerd proces is waarbij niet bepaalde groepen worden uitgesloten van registratie. Open bronnen staan tegenover afgeschermde bronnen die zich kenmerken doordat er een controle plaatsvindt op wie degene is die toegang wil tot de bron." O.a.: (2019). Internetonderzoek door bestuursorganen. *Nederlands Juristenblad, 94* (20), 1458-1466. / (2018). Regulering van opsporingsbevoegdheden in een digitale omgeving, p. 152./ (2018). 'Beschouwing rapport Commissie : strafvordering in het digitale tijdperk.' Platform Modernisering Strafvordering.

[33] (2021) Black Box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk. Pg 16-17

[34] (2021) Black Box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk.

[35] Article 29 Data Protection Working party, opinion 03/2013 on purpose limitation. III.2.5. & Annex II

[36] Zie hoofdstuk 3 en bijlage A.

dat het met *social monitoring* en -*scraping tools* verzamelen en hergebruiken van gegevens van deze gebruikers aan hun redelijke verwachtingen voldoet.

3.2.2 *Benodigde afweging bij gebruik tools*

Voor het raadplegen en gebruiken van informatie uit publiek toegankelijke bronnen gelden dus regels omdat dit inbreuk kan maken op de persoonlijke levenssfeer. Dit geldt ook voor het gebruik door de overheid, zoals Defensie, van *social media monitoring* of –*scraping tools*. Overheidsmaatregelen die inbreuk maken op artikel 8 van het EVRM kunnen zijn gelegitimeerd indien wordt voldaan aan de voorwaarden van artikel 8, tweede lid van het EVRM[37]. Dat hangt af van het bestaan van een grondslag voor die gedraging die bij wet is voorzien. Daarnaast moet ook worden gekeken naar het doel van een inbreuk. Dit doel moet kunnen worden aangemerkt als legitiem en noodzakelijk in een democratische samenleving. Wanneer sprake is van een legitiem doel, dient vervolgens te worden gekeken naar de (maatschappelijke) noodzaak van de voorgenomen inbreuk in verhouding tot dit legitieme doel. Hierbij speelt een rol of de voorgestelde inbreuk geschikt is om dat doel te bereiken en daarbij niet verder gaat dan noodzakelijk is (proportionaliteit), of minder ingrijpende middelen voorhanden zijn om hetzelfde resultaat te bereiken (subsidiariteit) en of afdoende waarborgen zijn ingesteld om disproportionele inbreuken en willekeur te voorkomen. Hierbij dient te worden aangetekend dat een dergelijke afweging niet eenvoudig is. Bijvoorbeeld: Je hebt een fantastische open dag op de kazerne gehad en in een tank gezeten. Je post dat met een foto op *social media* en schrijft er ook bij dat je wel dagelijks in een tank zou willen rijden. Is het dan vreemd als een defensieaccount je post leuk vindt? Is het dan vreemd als iemand van werving en selectie van Defensie contact met je opneemt omdat er vacatures zijn?

Uit het onderzoek komt naar voren dat bij de inkoop van *tools* of bij het in gebruik nemen van gratis *tools* meer aandacht nodig is voor privacyaspecten en de mate van inbreuk op de persoonlijke levenssfeer van betrokkenen. Wanneer persoonsgegevens uit publiek toegankelijke bronnen worden verwerkt, moet goed nagedacht worden over een legitiem doel en grondslag, en vervolgens of de verwerking ook echt noodzakelijk is. Per verwerking moet worden gekeken of de inzet van bevoegdheden niet verder gaat dan daadwerkelijk noodzakelijk en proportioneel is en of er een duidelijk beschreven doel is. Ook moet de intentie van de betrokkene, de subsidiariteit en of er effectieve maatregelen mogelijk zijn om de juistheid van gegevens te borgen en om disproportionele inbreuken te voorkomen worden afgewogen. Bij waarborgen tegen disproportionele inbreuken is de vraag ook in hoeverre in de praktijk een onderscheid gemaakt kan worden tussen ‘gesloten’ bronnen enerzijds en tussen ‘open’ bronnen anderzijds. Dit betekent ook dat bij gebruik van *tools* of bij het verkrijgen van geaggregeerde datasets bekend moet zijn uit welke bronnen de gegevens afkomstig zijn.

3.2.3 *Rechtmatigheid van de verwerking*

Voor een verwerking dient er een grondslag te zijn conform de Avg of Wpg. Voor verwerkingen die door Defensie worden uitgevoerd in het kader van haar taken betreft dit, in de context van het gebruik van *social monitoring* tools, een wettelijke verplichting of vervulling van een publieke taak (algemeen belang of openbaar gezag) waaruit een wettelijke grondslag te herleiden is voor het verwerken van persoonsgegevens. De grondslag voor een verwerking dient afgeleid te worden van een aan Defensie opgedragen taak, die het doel van de verwerking van persoons- of politiegegevens bepaalt. Een zelfstandige grondslag (taak en bevoegdheid) voor de

[37] There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

krijgsmacht voor het verzamelen en anderszins verwerken van persoonsgegevens voor operationele activiteiten kan alleen bestaan indien eenheden zijn ingezet op basis van een specifieke juridische grondslag. Het eerst verzamelen en daarna filteren, verwijderen of anonimiseren zijn allemaal verwerkingen waarvoor een grondslag vereist is. Voor de betrokkene moet het behoorlijk en transparant zijn hoe en waarom de persoonsgegevens verwerkt worden en waar ze vandaan komen als de betrokkenen ze niet zelf heeft verstrekt.

In de Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatieomgeving[38] wordt een algemeen overzicht gegeven van de meeste relevante juridische bepalingen die van toepassing zijn op de operationele activiteiten van de krijgsmacht in de informatieomgeving. Voor operationele taken van de krijgsmacht geven de juridische kaders maar beperkte mogelijkheden voor het gebruik van *tools* voor het verwerken van (persoons)gegevens van publiek toegankelijke bronnen waaronder *social media sites*.[39] Deze juridische kaders hebben geen betrekking op politietaken die de KMar uitvoert, waarvoor de politiewet 2012 als wettelijke basis geldt.

Bij een grotere (weloverwogen en afgestemde) behoefte, om *social monitoring* of –*scraping* toe te passen, dan dat het huidige juridische kader geeft, zal eerst onderzocht moeten worden of dit binnen de bestaande taakstelling en bevoegdheden van Defensie mogelijk is. Daarna kan bezien worden of aanvullende bevoegdheden nodig zijn. Hierbij moet ook gekeken worden naar welke verschillende rollen en taken reeds zijn toebedeeld aan defensie- en overheidsdiensten zoals de KMar, Politie en MIVD.

Overheidsinstanties kunnen zich bij het uitoefenen van hun *taken* niet baseren op de verwerkingsgrondslag van gerechtvaardigd belang[40]. Aangezien het aan de wetgever is om de rechtsgrond voor persoonsgegevensverwerking door overheidsinstanties te creëren, is de grondslag gerechtvaardigd belang niet van toepassing op de verwerking door overheidsinstanties in het kader van de uitvoering van hun taken. Er is voor het gebruik van gerechtvaardigd belang als wettelijke grondslag voor overheidsinstanties beperkt ruimte in het kader van behoorlijke beheer en de werking[41] van de organisatie. Dit betreft typische bedrijfsmatige handelingen[42] zoals het belang om de IT-infrastructuur goed te beveiligen en te beschermen of de beveiliging van overheidsgebouwen. Persoonsgegevens mogen dan verwerkt worden indien de verwerking noodzakelijk is voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen, met name wanneer de betrokkene een kind is. Er ontstaat dus een situatie waarin het recht van een organisatie 'botst' met het grondrecht van de betrokkenen. Het is aan de organisatie om deze rechten tegen elkaar af te wegen en te kijken wat zwaarder weegt, het belang van de organisatie of van dat van de betrokkenen. Deze afweging dient transparant te gebeuren.

3.2.4 Afweging bij verwerken van politiegegevens

De Wpg geeft aan dat politiegegevens enkel verwerkt mogen worden als dat rechtmatig en noodzakelijk is, maar dat creëert geen specifieke bevoegdheden ten

[38] Nota Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatieomgeving. Ministerie van Defensie / Directie Juridische Zaken. 12 april 2021.
[39] In bijlage A is een overzicht opgenomen van het van toepassing zijnde juridische kader.
[40] Artikel 6 lid 1 laatste zin Avg en overweging 45 Avg
[41] Working party 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC.
[42] Kamerstukken 2017-2018, 34 851, nr.3

aanzien van het rechtmatig verkrijgen van politiegegevens. Dergelijke bevoegdheden vloeien onder meer voort uit het Wetboek van Strafvordering, de Politiewet 2012 en de op deze wetten gebaseerde regelgeving of uit bijzondere wetten.[43] De Wpg geeft wel een aantal voorwaarden[44] aan voor het vergelijken van politiegegevens met andere dan politiegegevens. Gelet op het karakter van deze vorm van gegevensverwerking, die voor de persoonlijke levenssfeer ingrijpend kan zijn, dient de verantwoordelijke of de betrokken functionaris een zorgvuldige afweging te maken tussen het belang dat met de raadpleging is gediend en het belang van de personen van wie de gegevens kunnen worden betrokken.

Een belangrijk criterium in de strafvordering voor de mate van inbreuk die de toepassing van een bevoegdheid maakt, is de stelselmatigheid. Stelselmatigheid dient, op basis van vaste jurisprudentie van de Hoge Raad[45], te worden beoordeeld op basis van de combinatie van de verschillende handelingen en werkwijzen die uitgevoerd worden. Onderzoek op internet bestaat uit veel kleinere deelhandelingen, waardoor de mate waarin inbreuk wordt gemaakt door die handeling beperkt blijft. De combinatie van de verschillende handelingen kan echter samen toch een meer dan geringe inbreuk opleveren. Anders gezegd: als er op basis van de gecombineerde handelingen een 'min of meer volledig beeld van bepaalde aspecten van iemands privéleven' te verwachten is, is er sprake van stelselmatigheid en moet een bijzondere bevoegdheid worden gehanteerd. Op basis van jurisprudentie van de Hoge Raad geldt dit ook als het ontstaan van zo'n beeld reeds tevoren in redelijkheid is te verwachten[46].

3.3 Naleven Avg en Wpg

De minister van Defensie is voor de gehele defensieorganisatie de verwerkingsverantwoordelijke in de zin van de Avg en voor de politiegegevens die door de KMar worden verwerkt in de zin van de Wpg.
Via de Regeling Avg Defensie zijn de Avg-beheerders[47] belast met de zorg voor de naleving van de Avg en de wet ten aanzien van verwerkingen die gevoerd worden binnen het dienstonderdeel.
In de Regeling Wpg Defensie is de Commandant Koninklijke Marechaussee aangewezen als Wpg-beheerder. Politiegegevens mogen alleen worden verwerkt door defensiemedewerkers in de uitoefening van de politietaak of delen van de politietaak waarmee zij zijn belast en voor zover zij voor die verwerking zijn geautoriseerd door de Wpg-beheerder. Ten behoeve hiervan kan de Wpg-beheerder ook defensiemedewerkers die niet werkzaam zijn bij de KMar autoriseren om politiegegevens te verwerken.[48]

3.3.1 Register van verwerkingsactiviteiten

De verwerkingsverantwoordelijke (of-beheerder) dient Avg- en Wpg verwerkingen in een register van verwerkingsactiviteiten bij te houden. Ook verwerkingen vallend onder de RGMO en verwerkingen waarbij Defensie verwerker is dienen in een register te zijn opgenomen.[49] Geïnventariseerde *social monitoring*- of –scraping verwerkingen[50] waarbij persoonsgegevens worden verwerkt dienen opgenomen te zijn in het register van Defensie. Uit het onderzoek blijkt dat de geïnventariseerde verwerkingen niet of niet volledig zijn opgenomen in de registers. Daarmee is niet transparant en voldoende duidelijk vastgesteld voor welke doel en op basis van welk

[43] Kamerstukken II, 2005/06, 30 327, nr. 3, p. 3
[44] Zie artikel 11, lid 5, Wpg
[45] Kamerstukken II 1997/1998, 25403, nr. 3, p.26-28 en HR 21 maart 2000, ECLI:NL:PHR:2000:AA5254.
[46] Leidraad Bevoegdheden informatievergaring op internet - Opsporing Leeswijzer2, Openbaar Ministerie, 19 mei 2016.
[47] Plv SG, C-KMar, C-CZSK, C-CLSK, C-CLAS, C-DOSCO, C-DMO.
[48] Zie Wpg, artikel 1 lid a en k en artikel 6, en Regeling Wpg Defensie.
[49] Zie regeling Avg Defensie artikel 2.2
[50] Zie bijlage B

wettelijke grondslag persoonsgegevens worden verwerkt, welke categorieën persoonsgegevens worden verwerkt van welke categorieën betrokkenen, de bewaartermijnen van verzamelde persoonsgegevens enzovoort.

3.3.2 Wettelijke grondslag

Uit de eerste inventarisatie bleek dat vooral het vastleggen en onderbouwen van het doeleinde en de wettelijke grondslag van de verwerkingen ontbrak. Het risico bestaat dat door het ontbreken of niet volledig zijn van deze onderbouwing er onrechtmatige verwerkingen hebben plaatsgevonden. Naar aanleiding van het LIMC-onderzoek en de uitgevoerde inventarisatie zijn meerdere verwerkingen stopgezet omdat er mogelijk geen geldige wettelijke grondslag voor is. Daarnaast is gewerkt aan het onderbouwen en vastleggen (middels opstellen van een DPIA en vastleggen van de verwerking in het register) van doeleinde(n) en wettelijke grondslag van nog lopende verwerkingen, bijvoorbeeld voor communicatie of werving & selectie.

De wettelijke grondslag moet hoofdzakelijk gevonden worden binnen het juridisch kader van de uitvoering van de publieke taken of het gerechtvaardigd belang van de organisatie. Er is wel onduidelijkheid als het gaat om het opleiden, trainen en het oefenen met *social monitoring of –scraping tools* in het kader van de operationele gereedstelling. In theorie zou voor het opleiden in een oefenomgeving een fictieve dataset kunnen worden gebruikt. Aangegeven is dat voor het op een realistische wijze simuleren van inzet in het informatiedomein momenteel de technische en organisatorische mogelijkheden te beperkt zijn. Hierdoor kan in een aantal gevallen de operationele- en inzetgereedheid van eenheden met specifieke capaciteiten onvoldoende worden gegarandeerd.

3.3.3 Verwerkersovereenkomsten en gebruikersvoorwaarden

Er blijkt sprake van verwerkers (en sub-verwerkers) bij verschillende *tools*. Daar waar derde partijen persoonsgegevens ten behoeve van Defensie verwerken dient een verwerkersovereenkomst opgesteld te zijn. Het door derde partijen laten uitvoeren van bijvoorbeeld *social monitoring* activiteiten en laten ontdoen van persoonsgegevens ontslaat Defensie, als opdrachtgever, niet van de verwerkingsverantwoordelijkheid. Tevens is van belang om bij gebruik van *tools* de gebruikersvoorwaarden te beoordelen en de afweging vast te leggen.

Tijdens het onderzoek zijn niet alle verwerkersovereenkomsten of -afspraken en analyse van de toepasselijke gebruikersvoorwaarden aangetroffen. Hierdoor is niet volledig inzichtelijk welke afspraken gelden met verwerkers en of de toepasselijke gebruikersvoorwaarden zijn beoordeeld en in de praktijk worden nageleefd.

3.3.4 Data Protection Impact Assessment (DPIA)

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen dan dient voorafgaand aan de verwerking een DPIA uitgevoerd te worden. Uit ons onderzoek blijkt niet dat voor de geïnventariseerde verwerkingen voorafgaand een afweging is gemaakt of een DPIA noodzakelijk is. Er zijn voor de geïnventariseerde verwerkingen ten tijde van het onderzoek geen of geen actuele DPIA's aangetroffen. Ook hier ziet de FG dat verbeteringen worden getroffen. Voor gebruik van monitoring *tools* door Communicatieafdelingen wordt gewerkt aan een DPIA. De KMar is bezig met het actualiseren van de OSINT DPIA[51]. Voor het gebruik van *social monitoring* door werving en selectie en voor de bescherming van de IT-infrastructuur van Defensie zijn recentelijk DPIA's vastgesteld.

[51] DPIA Webint, Staf KMar/Juridische Zaken, mei 2018.

4 Werkzaamheden

4.1 Onderzoeksmethode

De uitvoering van dit onderzoek is vastgelegd in een plan van aanpak dat is vastgesteld door de opdrachtgever: de functionarissen voor gegevensbescherming Defensie. Door middel van de memo van 6 juli 2021, referentie BS2021015452, onderwerp "FG-onderzoeksopdracht *social monitoring tools* binnen Defensieonderdelen" hebben de FG's de betrokken commandanten, de Avg-coördinatoren, de hoofden Inkoop en hoofden Finance & Control geïnformeerd.

Voor dit onderzoek is gebruik gemaakt van een onderzoekskader gebaseerd op de relevante eisen uit de Avg, Wpg en andere gegevensbeschermingsbepalingen, en relevante juridische bepalingen voor het gebruik van *social monitoring*.

Uitgevoerde werkzaamheden bevatten onder meer: het uitvoeren van een inventarisatie die uitgezet is via de Avg-coördinatoren, interviews met medewerkers en analyse van de verkregen en verzamelde documenten en informatie en deelwaarnemingen van *tools* die gebruikt worden.

De uitvoering van werkzaamheden heeft plaatsgevonden van juli 2021 tot en met december 2021. De interviews zijn gehouden in oktober en november 2021.

4.1.1 Inventarisatie

De onderzoekers hebben hun verzoeken om informatie in de organisatie uitgezet via de lijnorganisatie. Via de Avg-coördinatoren is een verzoek gekomen aan Defensie om te inventariseren of er *social monitoring*-activiteiten worden uitgevoerd en welke *tools* hiervoor worden gebruikt. Het uitvoeren van een inventarisatie als onderdeel van het onderzoek was noodzakelijk omdat de betreffende processen niet of niet volledig in het register van verwerkingsactiviteiten zijn opgenomen.

Naast een inventarisatieverzoek bij de onderdelen van Defensie, is ook informatie gezocht op intranet, is het Defensie register van verwerkingsactiviteiten doorzocht en is informatie gezocht over *tools* en *social monitorin*g. Ook is informatie opgevraagd bij contacten in andere EU-landen met betrekking tot beschikbaarheid van juridische kaders en ervaringen met gebruik van *tools*.

Gelijktijdig heeft een analyse plaatsgevonden van het begrip (persoons)gegevens, politiegegevens, de kaders die worden gesteld vanuit de Wpg en de Avg, richtlijnen van het EDPB en van toepassing zijnde jurisprudentie. Naast interviews en deelwaarnemingen van *tools* die gebruikt worden is informatie opgevraagd bij gebruikers, Inkoop en Avg-coördinatoren en Wpg-privacyfunctionaris.

4.2 Rapportage

De conceptrapportage is voor hoor en wederhoor afgestemd met de Avg-coördinatoren van de defensieonderdelen en Wpg privacyfunctionaris. De conceptrapportage is ter review aangeboden aan een medewerker van de Directie Juridische Zaken.

Bijlage A : Toetsingskader

A.1 Is de Avg of Wpg van toepassing?

De Avg is van toepassing wanneer er sprake is van een geheel of gedeeltelijke geautomatiseerde verwerking van persoonsgegevens. Daarnaast is de Avg van toepassing op de handmatige verwerking van persoonsgegevens die in een bestand zijn of worden ogenomen.
Om te bepalen of de Avg van toepassing is moet vastgesteld worden of:

- gegevens worden verwerkt.
- in de gegevens persoonsgegevens zijn opgenomen.
- deze gegevens geheel of gedeeltelijk geautomatiseerd worden verwerkt, of ze zijn of moeten worden opgenomen in een bestand.
- de verwerking binnen het toepassingsbereik van de Avg valt.

Binnen de defensieorganisatie is de Wpg van toepassing bij de verwerking van persoonsgegevens in het kader van de politietaak bedoeld in het artikel 4 van de politiewet 2012 door de aangewezen ambtenaren van de KMar en in het kader van de uitvoering van de specifieke taken door de buitengewone opsporingsambtenaren (boa's), met uitzondering van de taken die aan de KMar zijn opgedragen vanuit de Vreemdelingenwet 2000 en enkele taken voor justitie (Avg van toepassing). De Wpg is van toepassing op de verwerking van politiegegevens die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen.

A.1.1 Verwerking

De Avg definieert een verwerking als iedere bewerking of geheel van bewerkingen met betrekking tot persoonsgegevens. Bijvoorbeeld persoonsgegevens verzamelen, opslaan, bijwerken, raadplegen en doorzenden.[52] Ook enkel data raadplegen en/of analyseren betreft een verwerking in de zin van de Avg.

De Wpg hanteert eenzelfde definitie m.a.w. een verwerking is elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens[53].

De definitie voor een verwerking is ruim opgezet: het verzamelen van persoonsgegevens zonder deze op te slaan, wordt al als een verwerking gedefinieerd. Een exploitant van een zoekmachine die gegevens verzamelt en deze via zijn indexeringsprogramma's opvraagt, vastlegt en ordent, op zijn servers bewaart en verstrekt of ter beschikking stelt van zijn gebruikers in de vorm van resultatenlijsten van hun zoekopdrachten is bezig met het verwerken van persoonsgegevens[54]. Ook het tijdens of voorafgaand aan het analyse- en productieproces verwijderen van persoonsgegevens uit de rapporten (pseudonimiseren of anonimiseren) is een verwerking van persoonsgegevens. Er is dus snel sprake van verwerken van persoonsgegevens als bedoeld in de Avg of de Wpg.

A.1.2 Persoonsgegevens en politiegegevens

In de Avg en de Wpg is een persoonsgegeven gedefinieerd als alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[55] Als identificeerbaar wordt beschouwd een natuurlijke persoon die direct (bijvoorbeeld aan de hand van

---

[52] Zie artikel 4, onder 2, Avg.
[53] Zie artikel 1, onder c, Wpg.
[54] HvJ EU 13 mei 2014, C-131/12, ECLI:EU:C:2014:317 (*Google Spain SL*), r.o. 28. (2021) Black Box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk.
[55] Zie artikel 4, aanhef en onder 1, Avg en artikel 2, onder b, Wpg.

een naam, adres, telefoonnummer), of indirect (bijvoorbeeld met behulp van een klantnummer, autokenteken) kan worden geïdentificeerd.[56] Van een persoonsgegeven is dus 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 inachtneming van de beschikbare technologie op het tijdstip van verwerking, maar ook de technologische ontwikkelingen in de nabije toekomst.

Ook als het gegevens zijn die niet tot concrete personen herleidbaar zijn, dient er wel nagegaan te worden of door koppeling van gegevens alsnog een natuurlijk persoon te identificeren is. De definitie van 'persoonsgegevens' wordt door de Europese rechters zo ruim opgevat, dat zodra er maar enige feit of omstandigheid is die zou kunnen leiden tot identificatie naar persoon, er sprake is van persoonsgegevens. Bij het gebruik van *social media monitoring* of *–scraping tools* is derhalve al gauw sprake van het verwerken van persoonsgegevens.

Een politiegegeven[57] is elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012. Dit met enkele uitzonderingen, zoals de taken in het kader van de Vreemdelingenwet 2000. Over wat een politiegegeven precies is, heeft de Afdeling bestuursrechtspraak van de Raad van State zich meermaals uitgelaten. Bij de beoordeling of gegevens als politiegegevens dienen te worden aangemerkt, is onder meer bepalend of die gegevens een geïdentificeerde of identificeerbare natuurlijke persoon betreffen. Daarbij dient te worden beoordeeld of die gegevens alleen of in combinatie met andere gegevens zo kenmerkend zijn voor die persoon, dat deze daarmee kan worden geïdentificeerd. Bij deze beoordeling mogen alle middelen worden betrokken waarvan mag worden aangenomen dat zij redelijkerwijs door de verantwoordelijke dan wel enig ander persoon zijn in te zetten om die persoon te identificeren.[58]

Voorbeelden van persoonsgegevens zijn: naam, voorvoegsel, adres, telefoonnummer, e-mailadres, leeftijd, geboortedatum en -plaats, geslacht, woonplaats, nationaliteit, IP-adres, MAC-adres, KvK-nummer, signalementsgegevens, gevarenclassificatie, voertuigidentificatienummer, winst eenmanszaak, bankrekeningnummer en -saldo, IQ, functie, opleiding, inkomens- en vermogensgegevens, kredietwaardigheid, persoonlijke voorkeuren, loonschaal, verslag van een functioneringsgesprek en (wan)gedrag. Ook metadata, bijvoorbeeld welke browser of telefoon iemand gebruikt, zijn persoonsgegevens als hieruit de identiteit van de betrokkene kan worden herleid. Ook locatie-informatie en geografische informatie kwalificeren als persoonsgegevens als de informatie herleidbaar is tot een persoon. Het maakt geen verschil dat een verantwoordelijke een gegeven niet zal gebruiken om een persoon mee te identificeren. Het feit dat de mogelijkheid bestaat bij de verantwoordelijke of bij een derde om dit te doen, is voldoende.

---

[56] 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".
[57] Zie artikel 1, onder a, Wpg
[58] Kamerstukken II 1997/98, 25 892, nr. 3, blz. 45-50; ABRvS 28 januari 2015, ECLI:NL:RVS:2015:224; van 29 september 2010, ECLI:NL:RVS:2010:BN8578

A.1.3 *Geautomatiseerd en/of handmatige verwerking*

Voor zowel de Avg als de Wpg geldt dat ze van toepassing zijn wanneer er sprake is van:

- een geheel of gedeeltelijk[59] geautomatiseerde verwerking van persoonsgegevens; of
- wanneer persoonsgegevens opgenomen zijn in een bestand[60] of die bestemd zijn om daarin te worden opgenomen.

De reikwijdte is dus niet afhankelijk van de gebruikte technieken.

Een aantal voorbeelden van (gedeeltelijk) geautomatiseerde verwerkingen zijn in de toelichting bij de Wet bescherming persoonsgegevens (Wbp) opgesomd, waaronder zoekopdrachten uitvoeren 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 opslaan, zoals 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."

A.1.4 *Toepassingsbereik van de Avg*

De Avg en de Uitvoeringswet Avg (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.

De geldende uitzonderingen zijn opgenomen in de RGMO. De Avg en de RGMO vormen het nationaalrechtelijk kader dat van toepassing is op militaire operaties. Aangezien overeenkomstige toepassing van de Avg het uitgangspunt is, zijn de uitzonderingen in de RGMO alleen gericht op de taakuitvoering, voor zover dat noodzakelijk is voor de vervulling van het mandaat en de bescherming van de (internationale) troepenmacht.[61] In het RGMO staan een aantal uitzonderingen op het verbod op het verwerken van bijzondere persoonsgegevens en op de rechten van betrokkene. Daarnaast kent de RGMO een aantal aanvullende bepalingen over bijzondere persoonsgegevens (biometrie en DNA), doorgifte, verdere verwerking en de bewaartermijn van persoonsgegevens.

---

[59] 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.

[60] Zie artikel 4, onder 6, Avg en artikel 1 lid o, Wpg: 'bestand": elk gestructureerd geheel van persoonsgegevens (Wpg: politiegegevens) die volgens bepaalde criteria toegankelijk zijn, ongeacht of dit geheel gecentraliseerd of gedecentraliseerd is dan wel op functionele of geografische gronden is verspreid."

[61] 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) 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."

Tijdens operaties worden ook persoonsgegevens verwerkt waarvoor de uitzonderingen niet van toepassing zijn omdat deze verwerkingen niet noodzakelijk zijn voor de vervulling van het mandaat en de bescherming van de (internationale) troepenmacht[62]. Hierop is de Avg van toepassing.

Daarnaast bestaat er voor Defensie een uitzondering, uit hoofde van artikel 3, derde lid, onder a en b, UAvg, als de Wet op de inlichtingen- en veiligheidsdiensten 2017 van toepassing is op de verwerking van persoonsgegevens. In de Wiv staan de bijzondere bevoegdheden beschreven die de MIVD mag inzetten. De verwerking van persoonsgegevens in het kader van de Wiv valt buiten de scope van dit onderzoek.

A.1.5 *Toepassingsbereik Wpg*

Uitgezonderd van de Avg is ook de verwerking van persoonsgegevens door de bevoegde autoriteiten, waaronder de KMar, 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[63]. Op deze activiteiten is de Europese richtlijn 2016/680/EG van toepassing. In Nederland is deze Richtlijn geïmplementeerd in de Wpg en de Wet Justitiële en strafvorderlijke gegevens (Wjsg). Voor wat betreft het toepassingsbereik sluiten de Avg en de richtlijn elkaar wederzijds uit: waar de richtlijn geldt is de Avg niet van toepassing en andersom.[64] De aard van het werk van politie- en opsporingsdiensten, waaronder de KMar, brengt met zich mee dat gegevens over burgers zonder hun medeweten moeten kunnen worden verzameld.[65] Bij de verwerking van politiegegevens gaat het telkenmale om de bescherming van de privacy van de individuele burger c.q. rechtspersoon afgewogen *ten opzichte van* het belang van een effectieve rechtshandhaving.

A.1.6 *Geanonimiseerde of gepseudonimiseerde gegevens*

Bij pseudonimisering worden identificerende gegevens gescheiden van niet-identificerende gegevens en vervanging door kunstmatige identificatoren. Omdat er een koppeling tot stand kan worden gebracht tussen de gepseudonimiseerde gegevens en identificerende gegevens, zijn gepseudonimiseerde gegevens onverkort persoonsgegevens. De Avg is dan ook volledig van toepassing op gepseudonimiseerde gegevens. De pseudonimisering fungeert als een maatregel om persoonsgegevens te beschermen en te beveiligen.

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 geen sprake meer van verwerking van persoonsgegevens. De gegevens dienen wel daadwerkelijk anoniem te zijn en er mag geen mogelijkheid zijn tot identificatie door bijvoorbeeld herleiding, koppeling of deductie.

Het anonimiseren op zichzelf is overigens al een verwerking van persoonsgegevens.[66] In de praktijk betekent het dat het feitelijk niet mogelijk is gegevens te ontdoen, of door een derde partij te laten ontdoen, van hun identificeerbaarheid, zonder dat een privacywet van toepassing is.

A.2 Voorwaarden voor rechtmatige verwerking van persoonsgegevens

Indien de Avg of de Wpg van toepassing is dient de concrete gegevensverwerking in overeenstemming te zijn met de regels uit de Avg of Wpg.

---

[62] Zie verder: 0903-DOPS-SOP ED-Verwerken persoonsgegevens tijdens operaties. 01-05-2018
[63] Zie artikel 2, tweede lid, onder d, Avg
[64] Kamerstukken II 2017/18, 34 889, 3, p.3
[65] Kamerstukken I 2006/07, 30327, C, p. 22
[66] Overweging 26 Avg en overweging 21 Richtlijn

De Avg schrijft voor dat persoonsgegevens rechtmatig, behoorlijk en transparant worden verwerkt. De Wpg schrijft eveneens voor dat de gegevens behoorlijk en rechtmatig verkregen moeten zijn en dat de gegevens, gelet op de doeleinden waarvoor zij worden verwerkt toereikend, ter zake dienend en niet bovenmatig zijn.

De Wpg regelt geen bevoegdheden over de wijze waarop politiegegevens kunnen worden verkregen. Dergelijke bevoegdheden vloeien onder meer voort uit het Wetboek van Strafvordering, de Politiewet 2012 en de op deze wetten gebaseerde regelgeving of uit bijzondere wetten zoals de Wet op de economische delicten.

A.2.1 *Rechtmatige verwerking Avg: rechtsgrondslag*

Een verwerking van persoonsgegevens vindt plaats voor een gerechtvaardigd doel, voor zover deze kan worden gebaseerd op een van de grondslagen zoals bedoeld in artikel 6 Avg[67] en het doeleinde in overeenstemming is met de toepasselijke wet- en regelgeving.

Van de in artikel 6 Avg genoemde wettelijke grondslagen zijn voor verwerkingen die door Defensie worden uitgevoerd over het algemeen en in de context van het gebruik van *social monitoring* maar een deel van toepassing, namelijk:

- de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
- 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;
- de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

Daarnaast is de 'noodzakelijkheidsgrondslag' van belang: alleen wanneer de verwerkingen noodzakelijk zijn voor de in deze grondslag genoemde doelen, dan is de verwerking gerechtvaardigd. Bij de afweging van de noodzakelijkheid moet afgewogen worden of de verwerking van gegevens proportioneel is en voldoet aan de eis van subsidiariteit.

Een wettelijke grondslag hebben voor een publieke taak betekent volgens de wetgever niet dat de wettelijke grondslag voor de gegevensverwerking een 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[68], 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 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".

4.2.1.1 Wettelijke verplichting

Een verwerking is rechtmatig als deze noodzakelijk is om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijk rust[69]. Het is niet noodzakelijk dat de wettelijke verplichting als zodanig is vastgelegd in een wet in formele zin. Wel moet de wetgevingsmaatregel, overeenkomstig de rechtspraak van

[67] Als bedoeld in artikel 6, eerste lid, Avg.
[68] Kamerstukken II 2017/18, 34 851, nr. 3, p. 35-36 (inzake de 'gewone grondslag' in de zin van artikel 6 Avg
[69] Avg, overweging 40

het Hof van Justitie (HvJ) EU en het Europees Hof voor de Rechten van de Mens (EHRM) duidelijk en nauwkeurig zijn, en de toepassing daarvan moet voorspelbaar zijn voor degenen op wie deze van toepassing is[70]. Een verplichting tot verwerking van persoonsgegevens in lagere regelgeving moet (uiteraard) wel een basis hebben in een wet in formele zin. De wettelijke verplichting moet worden vastgesteld op het niveau van de unie of een lidstaat. Een op de verwerkingsverantwoordelijke rustende verplichting tot gegevensverwerking op grond van de wetgeving van landen buiten de EU kan als zodanig geen rechtsgrond vormen voor de gegevensverwerking[71].

De verordening schrijft niet voor dat voor elke afzonderlijke verwerking specifieke wetgeving vereist is. Er kan worden volstaan met wetgeving die als basis fungeert voor verscheidene verwerkingen. De verwerking van persoonsgegevens kan ook een basis vinden in een ruimer geformuleerde wettelijke zorgplicht. In dat geval heeft de verwerkingsverantwoordelijke een grotere eigen verantwoordelijkheid bij het beoordelen van de noodzakelijkheid van de verwerking in het licht van het voldoen aan de wettelijke verplichting. In de wetgeving wordt het doel van de verwerking vastgesteld. Daarnaast kan de wetgeving een nadere invulling geven aan de algemene voorwaarden waaraan de gegevensverwerking moet voldoen om rechtmatig te zijn, bijvoorbeeld door specificatie van de entiteiten waaraan de persoonsgegevens mogen worden vrijgegeven en de bewaartermijn.[72]

4.2.1.2 Taak van algemeen belang of taak in het kader van de uitoefening van het openbaar gezag

Een verwerking is rechtmatig als deze noodzakelijk is voor de vervulling van een publieke taak van algemeen belang of de uitoefening van openbaar gezag dat aan de verwerkingsverantwoordelijke is toevertrouwd. De publieke taak hoeft niet uitputtend geregeld te zijn in een wet in formele zin. Voldoende is dat de hoofdlijnen kenbaar zijn uit de sectorspecifieke wetgeving die op de verwerkingsverantwoordelijke van toepassing is. Er kan worden volstaan met een samenstel van wettelijke regels die tezamen een publieke taak aanduiden. Het doel van de verwerking moet noodzakelijk zijn voor de vervulling van een publieke taak. De ruimte voor gegevensverwerking vindt hierin zijn begrenzing De wetgeving kan voorts een nadere invulling geven aan de algemene voorwaarden voor rechtmatige gegevensverwerking, bijvoorbeeld door specificatie van het type persoonsgegevens, de betrokkenen, de entiteiten waaraan de persoonsgegevens mogen worden verstrekt, de doelbinding, de bewaartermijn en andere maatregelen om te zorgen voor de rechtmatige en behoorlijke verwerking.[73]

Om verwerkingen van persoonsgegevens op de grondslag te mogen baseren, moet het niet mogelijk zijn om het doel te realiseren zonder dat er persoonsgegevens moeten worden verwerkt.

4.2.1.3 Gerechtvaardigd belang

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.

---

[70] Avg, overweging 41
[71] Privacy- en gegevensbeschermingsrecht. AVG, UAVG en andere privacywetgeving. Zevende druk. . Pg 95.
[72] Privacy- en gegevensbeschermingsrecht. AVG, UAVG en andere privacywetgeving. Zevende druk. . Pg 96.
[73] Privacy- en gegevensbeschermingsrecht. AVG, UAVG en andere privacywetgeving. Zevende druk. . Pg 96-97.

Om verwerkingen op deze grondslag te kunnen baseren, moet zorgvuldig beoordeeld worden of er sprake is van een gerechtvaardigd belang, maar ook om te bepalen of de betrokkene, gelet op het moment en de context van de verzameling van de persoonsgegevens, redelijkerwijs mag verwachten dat zijn persoonsgegevens voor dit doel worden verwerkt.

Overheidsinstellingen mogen zich bij het uitoefenen van *hun taken* nooit beroepen op de grondslag van gerechtvaardigd belang. Wat ook niet mag is zelf de bevoegdheden uitbreiden op grond van het gerechtvaardigd belang.

Voor zover het gaat om het *behoorlijke beheer en de werking*[74] van de organisatie is er is voor overheidsinstanties wel – zij het beperkt – ruimte voor het gebruik van gerechtvaardigd belang als wettelijke grondslag voor het verwerken van persoonsgegevens. Dit betreft dan typische bedrijfsmatige handelingen[75] zoals bijvoorbeeld de registratie en administratie van het wagenpark.

Op basis van de normuitleg 'gerechtvaardigd belang' van de AP[76] moet worden afgewogen of:

- Het belang rechtmatig is. Is het in overeenstemming met toepasselijk EU- en nationaal recht? Het belang dat wordt nastreeft moet passen binnen de kaders van de wetten.
- Het belang voldoende duidelijk en specifiek verwoord is. Het belang dient zo concreet mogelijk beschreven te zijn.
- Er sprake is van een 'echt' en dus niet 'speculatief' belang. Het belang moet zich in het hier en nu bevinden. Persoonsgegevens mogen niet verwerkt worden met de veronderstelling dat de organisatie hier mogelijk in de toekomst baat bij kan hebben.
- Een betrokkene redelijkerwijs kan verwachten dat deze gegevens voor het door gekozen doel verwerkt kunnen worden (*reasonable expectation of privacy)*.
- Er (aanvullende) waarborgen getroffen kunnen worden om ongewenste gevolgen voor de betrokkene te voorkomen of te beperken.

Wanneer een verwerking is gebaseerd op gerechtvaardigd belang, dan dient dit transparant te gebeuren. Het moet duidelijk zijn voor welke doelen persoonsgegevens worden verwerkt, welke persoonsgegevens worden verwerkt, of de gegevens worden gedeeld met andere partijen en hoe lang de persoonsgegevens worden bewaard.

A.2.2 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[77], worden deze taken op de volgende wijze uitgewerkt:

[74] Working party 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of Directive 95/46/EC.
[75] Kamerstukken 2017-2018, 34 851, nr.3
[76] Autoriteit Persoonsgegevens 1 november 2019 normuitleg grondslag gerechtvaardigd belang
[77] Raadpleegbaar via https://www.defensie.nl/downloadslbeleidsnota-s/201 8103126/defensienota-2018

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.[78] Uit artikel 97 Grondwet vloeit als zodanig dus geen - zelfstandig werkende - taak of bevoegdheid voort voor de krijgsmacht. Met andere woorden: de krijgsmacht mag zichzelf geen taken op grond van artikel 97, eerste lid, Grondwet, toebedelen en daarmee zichzelf inzetten.

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)[79].

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 KMar en de taak van de krijgsmacht die is belegd in de Rijkswet Geweldgebruik Bewakers Militaire Objecten.

Bij 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. De krijgsmacht heeft daarbij geen eigen bevoegdheden, maar taken en bevoegdheden van het ondersteunde civiele gezag. Dat betekent derhalve dat het civiele gezag de verwerkingsverantwoordelijke is. Het civiele gezag bepaalt de doeleinden waarvoor en de middelen waarmee persoonsgegevens worden verwerkt. 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.

[78] Zie Kamerstukken 111997/98, 25367 (R 1593), nr. 3, p. 3
[79] Zie de Regeling inzake militaire steunverlening in het openbaar belang.

Bij internationale inzet worden bevoegdheden gebaseerd op de internationaalrechtelijke grondslag voor de inzet, binnen de grenzen van mensenrechten en andere toepasselijke internationaalrechtelijke verplichtingen.

i) bij inzet op grond van uitoefening van het statelijke recht op (collectieve) zelfverdediging, worden de bevoegdheden bepaald door de reikwijdte van het statelijke recht op zelfverdediging en het humanitair oorlogsrecht;
ii) bij inzet op grond van een mandaat van de VN-Veiligheidsraad, worden de bevoegdheden bepaald door de autorisaties die de VN-Veiligheidsraad geeft;
iii) bij inzet op grond van de instemming van een gastland, worden de bevoegdheden bepaald door de reikwijdte van de instemming van dat gastland. Toestemming van een gastland biedt echter geen zelfstandige grondslag voor bevoegdheden.

Bij inzet op grond van uitoefening van het statelijke recht op (collectieve) zelfverdediging mogen persoonsgegevens verwerkt worden voor zover dat binnen de grenzen van het oorlogsrecht en mensenrechten noodzakelijk is voor de uitoefening van zelfverdediging. De RGMO is van toepassing.
Bij een mandaat van de VN-Veiligheidsraad zijn de bevoegdheden afhankelijk van de vraag of het een VN-gemandateerde operatie of een VN-geleide operatie is. Als er sprake is van een VN gemandateerde operatie, mogen persoonsgegevens worden verwerkt voor zover dat binnen de grenzen van het VN-mandaat en mensenrechten noodzakelijk is voor de uitvoering van het mandaat. Als er sprake is van een VN-geleide operatie, vindt eventuele verwerking van persoonsgegevens plaats onder verantwoordelijkheid van de VN en zijn de VN-bepalingen daarop van toepassing.

Bij gereedstelling ten behoeve van dergelijke inzet is het mogelijk om onder voorwaarden gebruik te maken van dezelfde bevoegdheden die van toepassing zijn op de daadwerkelijke inzet. Een belangrijke voorwaarde is dat er een grondslag is voor de geplande operatie en dat er een regeringsbesluit is tot inzet. Dat betekent dat de periode beperkt is waarin gebruik gemaakt kan worden van deze mogelijkheid.

Vereenvoudigd schematisch overzicht bij de Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatieomgeving

	Grondslag/aard van de activiteit	***Nationale grondslag***	***AVG***
1	*Statelijk recht op (collectieve) zelfverdediging*	*Regeringsbesluit*	*Avg 'publieke taak' (art 6.1.3) RGMO*
2.a	*VN-gemandateerde operatie*	*Regeringsbesluit (art.100)*	*Avg 'publieke taak' (art 6.1.3) RGMO*
2.b	*VN-geleide operatie*	*Regeringsbesluit (art.100)*	*n.v.t.*
3	*Instemming gastland*	*Regeringsbesluit (evt. art 100)*	*Afhankelijk van de aard van de inzet/activiteit*
4	*Inzet zonder specifieke juridische grondslag*	*Regeringsbesluit of besluit Mindef*	*Evt. Avg 'toestemming' (art. 6.1.a)*
5	*MB/MSOB*	*Politiewet, Wet veiligheidsregio's, MSOB, etc.*	*Verwerkersovereenkomst*
6	*Specifieke gereedstelling*	*Regeringsbesluit*	*Volgt operatie*
7	*Algemene gereedstelling*	*n.v.t*	*Evt. Avg 'toestemming' (art. 6.1.a)*

A.2.3 De publieke taken van de Minister van Defensie

Naast de taken die opgedragen zijn aan de krijgsmacht zijn er verschillende wetten waaruit een verplichting vloeit voor Defensie zoals de Wet Ambtenaren Defensie, de Aanbestedingswet op Defensie- en Veiligheidsgebied, de Luchtvaartwet, de Veteranenwet, de Wet Immunisatie Militairen en de Wet open overheid.

A.2.4 *Legitieme rechtsgrond: Wpg*

Voor de verwerking van politiegegevens is het doel bij wet omschreven. De wet heeft die gecategoriseerd in de uitvoering van de dagelijkse politietaak (artikel 8), het onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9), inzicht in de betrokkenheid van personen bij bepaalde ernstig bedreigingen van de rechtsorde (artikel 10), het beheer van informanten (artikel 12) en de gegevensverwerking voor landelijke ondersteunende taken (artikel 13).

De Wpg geeft aan dat politiegegevens enkel verwerkt mogen worden als dat rechtmatig en noodzakelijk is, maar dat creëert geen specifieke bevoegdheden ten aanzien van het rechtmatig verkrijgen van politiegegevens. Dergelijke bevoegdheden vloeien onder meer voort uit het Wetboek van Strafvordering, de Politiewet 2012 en de op deze wetten gebaseerde regelgeving of uit bijzondere wetten.[80] De Wpg geeft wel een aantal voorwaarden aan voor het vergelijken van politiegegevens met andere dan politiegegevens. Artikel 11, vijfde lid, van de Wpg geeft de mogelijkheid om politiegegevens die worden verwerkt op grond van de artikelen 8[81], 9[82] of 10[83] geautomatiseerd te vergelijken met andere dan politiegegevens voor zover dit noodzakelijk is voor een artikel 9, eerste lid (recherche onderzoek) of een artikel 10, eerste lid, verwerking.

A.2.5 *Het Europees Verdrag voor de Rechten van de Mens*

Artikel 8 van het EVRM beschrijft het recht op eerbiediging van privé-, familie- en gezinsleven. Inmenging in de uitoefening van dit recht door overheidsmaatregelen kan enkel gelegitimeerd zijn als wordt voldaan aan de voorwaarden van artikel 8, tweede lid van het EVRM. Deze voorwaarden zijn:

- de doelen zoals genoemd in artikel 8, tweede lid van het EVRM wordt nagestreefd;
- de inbreuk 'bij wet is voorzien'; en
- de maatregel 'noodzakelijk is in een democratische samenleving'.

Zo moet worden gekeken naar het doel van een inmenging. Dit doel moet kunnen worden aangemerkt als "legitiem" in een democratische samenleving. Wanneer sprake is van een legitiem doel, dient vervolgens te worden gekeken naar de (maatschappelijke) noodzaak van de voorgenomen inmenging in verhouding tot dit legitieme doel. Hierbij speelt een rol of de voorgestelde inbreuk geschikt is om dat doel te bereiken en daarbij niet verder wordt gegaan dan noodzakelijk is (proportionaliteit), of minder ingrijpende middelen voorhanden zijn om hetzelfde resultaat te bereiken (subsidiariteit) en of afdoende waarborgen zijn ingesteld om disproportionele inbreuken en willekeur te voorkomen.

A.3 Beginselen en bepalingen

Artikel 5 van de Avg en artikelen 3 en 4 van de Wpg geven een aantal algemene beginselen die moeten worden nageleefd, zoals doelbinding en noodzakelijkheid.

A.3.1 *Avg: Doelbinding*

Persoonsgegevens moeten[84] 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 te zijn vastgelegd

[80] Kamerstukken II, 2005/06, 30 327, nr. 3, p. 3
[81] Uitvoering van de dagelijkse politietaak.
[82] Onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (rechercheonderzoek).
[83] Inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde.
[84] Als bedoeld in artikel 5, aanhef en onder b, Avg.

wanneer de persoonsgegevens worden verzameld. De doeleinden dienen expliciet en gerechtvaardigd te zijn.

A.3.2 *Avg: Verdere verwerking van persoonsgegevens*

Wanneer persoonsgegevens later voor een ander doel worden verwerkt dan ze aanvankelijk zijn verzameld moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel.

Om te bepalen of een nieuw doel verenigbaar is, moet worden gekeken naar een aantal elementen[85]:

- Het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter de twee doelen bij elkaar liggen, hoe eerder de verdere verwerking van persoonsgegevens verenigbaar is met het oorspronkelijke doel.
- De context waarin de persoonsgegevens zijn verzameld. Hierbij moet met name worden gekeken naar de relatie met de betrokkene in kwestie en de redelijke verwachtingen die de betrokkene heeft ten aanzien van het verdere gebruik van zijn persoonsgegevens door de verwerkingsverantwoordelijke[86].
- De aard van de persoonsgegevens. Wanneer het bijvoorbeeld gevoelige persoonsgegevens betreft, geldt dat deze een hoger beschermingsniveau verdienen en dat deze minder snel voor andere doelen mogen worden gebruikt.
- De mogelijke gevolgen van de verdere verwerking voor betrokkenen.
- Het bestaan van passende waarborgen. Als de persoonsgegevens bijvoorbeeld zijn versleuteld of gepseudonimiseerd, zullen deze eerder voor andere doelen mogen worden gebruikt dan wanneer geen waarborgen zijn getroffen.

Als sprake is van een verenigbare verdere verwerking, dan is bij een interne verdere verwerking door dezelfde verwerkingsverantwoordelijke geen afzonderlijke wettelijke grondslag vereist. Bij een externe verdere verwerking (door een andere verwerkingsverantwoordelijke) dient de verwerkingsverantwoordelijke over een afzonderlijke wettelijke grondslag te beschikken[87].

Als 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).

A.3.3 *Wpg: Doelbinding*

Politiegegevens mogen slechts verwerkt worden voor zover dit noodzakelijk is voor de bij of krachtens de wet geformuleerde doeleinden. Voor de Wpg is het doel bij wet omschreven, namelijk de verwerking ten behoeve van de uitvoering van de politietaak. Politiegegevens worden slechts verwerkt voor welomschreven en gerechtvaardigde doelen en de verwerking van gegevens is evenredig aan het betreffende doel.

---

[85] Handleiding Algemene Verordening Gegevensbescherming, Ministerie van Justitie en Veiligheid

[86] Gegevensbeschermingsautoriteit: Dossiernr.: DOS-2018-04433. Beslissing ten gronde 13/2022 van 27 januari 02. Sanctie voor massale verwerking van Twitter-gegevens in verband met de affaire Benalla voor politieke profilering "Daarom moet in casu rekening worden gehouden met de verwachtingen van de betrokkenen: dit houdt in dat wanneer personen hun gegevens hebben bekendgemaakt aan een eerste verwerkingsverantwoordelijke (bv. Twitter) en redelijkerwijs niet verwachten dat die door een andere verwerkingsverantwoordelijke verder zullen worden verwerkt (bv. politieke profilering artikel 4, lid 4, van de Avg), een dergelijk hergebruik van gegevens voor nieuwe doeleinden enkel mogelijk is met hun toestemming, tenzij er een andere rechtsgrond is, zoals het gerechtvaardigde belang van de verwerkingsverantwoordelijke."

[87] Zie Kamerstukken II 2018/19, 34 851, nr. 3, p. 38

Politiegegevens mogen uitsluitend voor een ander doel verwerkt dan waarvoor zij zijn verkregen voor zover de Wpg daar uitdrukkelijk in voorziet, deze verwerking niet onverenigbaar is met het doel waardoor deze gegevens zijn verkregen en de verwerking voor dat andere doel overigens noodzakelijk is en in verhouding staat tot dat doel.

A.3.4 *Transparantie*

Wanneer het gerechtvaardigd is om persoonsgegevens te verwerken, dan moet de verwerking ervan vervolgens netjes en verantwoord gebeuren. Ten slotte moet duidelijk zijn voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt. Ook in gevallen waarin een verwerkingsverantwoordelijke zich op een gerechtvaardigd belang wil baseren, moet zorgvuldig gekeken worden naar de verplichting van transparantie en het recht op bezwaar.

A.3.5 *Noodzakelijkheid*

Persoonsgegevens en politiegegevens zijn toereikend, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt (dataminimalisatie).
Dit houdt in dat de verwerkingsverantwoordelijke enkel *need to know*-informatie mag verwerken, in plaats van *nice to know*-informatie.
Uit het noodzakelijkheidsbeginsel volgt dat de privacy inbreuk die gepaard gaat met een verwerking noodzakelijk moet zijn voor het doel waarvoor het wordt ingezet (proportionaliteit). De gegevens moeten nodig zijn om het doel te kunnen bereiken en de gegevens moeten in verhouding staan tot het doel. Daarnaast mag de verwerkingsverantwoordelijke slechts overgaan tot het verwerken van (strafrechtelijke of bijzondere) persoonsgegevens, als het onderzoeksdoel niet met minder vergaande maatregelen kan worden bereikt ('subsidiariteit'). Deze verplichting 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.

A.3.6 *Juistheid*

De verwerkingsverantwoordelijk 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 verwekte gegevens.

A.3.7 *Passende technische en organisatorische maatregelen*

De Avg en Wpg schrijven voor dat "passende technische en organisatorische maatregelen" worden getroffen ter beveiliging van de verwerking.

A.4 **Doorbrekingsgrond: kennelijk openbaar gemaakt door betrokkene**

Op grond van artikel 9, lid 2, punt e), Avg kunnen bijzondere categorieën van gegevens worden verwerkt wanneer de gegevens kennelijk door de betrokkene openbaar zijn gemaakt. Het woord "kennelijk" impliceert dat er een hoge drempel moet zijn om deze uitzondering te kunnen inroepen. De wetgever wijst er bij de toelichting op de soortgelijke bepaling in de Wbp[88] op dat de intentie van de betrokkene van belang kan zijn. Zo is geen sprake van uitdrukkelijke openbaarmaking als een betrokkene persoonsgegevens openbaar maakt via een afgeschermd (*social media*-) profiel[89]. De EDPB[90] merkt op dat de aanwezigheid van een enkel element niet altijd voldoende is om vast te stellen dat de gegevens kennelijk door de betrokkene openbaar zijn gemaakt.

[88] Zie Kamerstukken II 1997/98, 25 892, nr. 3, p.123
[89] Zie Kamerstukken II 1997/98, 25 892, nr. 3, p.123, en ook nr. 6, p.42.
[90] EDPB Richtsnoeren 8/2020 betreffende de targeting van gebruikers van sociale media.

In de praktijk moet door een verwerkingsverantwoordelijken mogelijk een combinatie van elementen worden overwogen om aan te tonen dat de betrokkene duidelijk zijn wil heeft geuit de gegevens openbaar te maken en moet een individuele beoordeling worden uitgevoerd. De volgende elementen kunnen relevant zijn bij deze beoordeling:

i) de standaardinstellingen van het *social media-platform*. Dat wil zeggen dat de betrokkene specifieke actie heeft ondernomen om deze persoonlijke standaardinstellingen te wijzigen in algemene instellingen; of

ii) de aard van het *social media-platform*. Dat wil zeggen of dit platform intrinsiek samenhangt met het idee om in contact te komen met naaste kennissen van de betrokkene of om een intieme relatie aan te gaan (zoals onlinedatingplatforms), dan wel of het platform is bedoeld om een breder scala aan interpersoonlijke relaties, zoals professionele relaties of sociale platforms voor het delen van online recensies; of

iii) de toegankelijkheid van de pagina waarop de bijzondere gegevens worden gepubliceerd. Bijvoorbeeld of de informatie openbaar toegankelijk is dan wel een account moet worden aangemaakt om toegang tot de informatie te krijgen; of

iv) de zichtbaarheid van de informatie waar de betrokkene wordt geïnformeerd over het openbare karakter van de informatie die hij publiceert. Kan bijvoorbeeld de betrokkene uit de knop voor publicatie afleiden dat de informatie openbaar wordt gemaakt; of

v) als de betrokkene gevoelige gegevens zelf openbaar heeft gemaakt of dat de gegevens door een derde openbaar zijn gemaakt of zijn afgeleid.

Met andere woorden, bij de beoordeling of de gegevens door de betrokkene kennelijk openbaar zijn gemaakt, moet rekening worden gehouden met de omstandigheden van het specifieke geval.

A.5 Verantwoording

De verwerkingsverantwoordelijke moet kunnen aantonen[91] dat de verplichtingen van de Avg en Wpg worden nageleefd wanneer persoonsgegevens worden verwerkt. In deze paragraaf volgt een bespreking van de belangrijkste formele verplichtingen uit de Avg en Wpg die uitvoering geven aan deze verantwoordingsplicht.

A.5.1 Verwerkingenregister

Een van de manieren om (deels) uitvoering te geven aan de verantwoordingseis is een verwerkingsregister[92]. In het verwerkingsregister staat informatie over de persoonsgegevens/politiegegevens die worden verwerkt. Dit betreft onder andere per verwerking het doel en rechtsgrond, de categorieën van personen waarover gegevens worden verwerkt, de categorieën van persoonsgegevens, de bewaartermijnen en of er sprake is van een verwerker.

De artikelen 2.1 en 2.2. van de Regeling Avg Defensie en het artikel 2.1 van de Regeling Wpg Defensie schrijven bovendien voor op welke wijze registratie dient plaats te vinden. Voor verwerkingen die vallen onder de RGMO[93] dient er ook een register van verwerkingsactiviteiten, zoals bedoeld in artikel 30 van de Avg, bijgehouden te worden.

A.5.2 DPIA – wanneer & waarvoor nodig

Wanneer een voorgenomen verwerking van persoonsgegevens waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, dan dient

[91] Dit volgt uit de in artikel 5, tweede lid, Avg opgenomen 'verantwoordingsplicht'. Zie ook §5 Wpg.
[92] Artikel 30 Avg en artikel 32d Wpg.
[93] Artikel 6, RGMO

voorafgaand aan de verwerking een zogenaamde gegevensbeschermingseffectbeoordeling[94], in de praktijk *Data Protection Impact Assessment* (DPIA) genoemd, uitgevoerd te worden. Tevens wordt een DPIA geïnitieerd bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien[95]. Een DPIA is bijvoorbeeld vereist wanneer er sprake is van een grootschalige verwerking van persoonsgegevens en/of stelselmatige monitoring waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen.

De Autoriteit Persoonsgegevens (AP) heeft een lijst[96] van verwerkingen opgesteld waarvoor het uitvoeren van een DPIA altijd verplicht is. Op basis hiervan is het waarschijnlijk dat voor alle verwerkingen waar *social media monitoring* plaatsvindt een DPIA vereist is.

Een DPIA is een instrument om de effecten voor betrokkenen op een gestructureerde en gestandaardiseerde wijze in kaart te brengen en te beoordelen, wordt de noodzaak beoordeeld en kunnen de aan de verwerking verbonden risico's beheerd worden.

Na het doorlopen van de DPIA moet het advies ingewonnen worden van de FG[97]. Het advies van de FG dient samen met de beslissingen van de verwerkingsverantwoordelijke in de DPIA te worden gedocumenteerd. Als de verwerkingsverantwoordelijke niet met het door de FG verleende advies instemt, wordt gemotiveerd waarom met het advies geen rekening is gehouden.[98]

A.5.3 *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 verwerker verwerkt persoonsgegevens in opdracht van een andere organisatie en gebruikt deze persoonsgegevens niet voor eigen doeleinden. Als een verwerkingsverantwoordelijke gebruik maakt van een verwerker[99] dient de verwerkingsverantwoordelijke door middel van (onder meer) een verwerkersovereenkomst of verwerkersafspraken (tussen overheidsorganisaties) te borgen dat de verwerker de vereisten van de Avg strikt naleeft.
Ook de Wpg-beheerder kan politiegegevens laten verwerken door een verwerker, met inachtneming van artikel 6c van de wet en artikel 6:1b van het Besluit politiegegevens. In dit geval dient de overeenkomst tot verwerking van de betreffende politiegegevens worden vastgelegd in een schriftelijke verwerkersovereenkomst tussen de verwerker en de Wpg-beheerder dit optreedt namens de minister.

[94] Zie artikel 35 Avg en artikel 4b Wpg
[95] Artikel 3, lid 1 onder b Regeling Avg Defensie
[96] Besluit inzake lijst van verwerkingen van persoonsgegevens waarvoor een gegevensbeschermingseffectbeoordeling (DPIA) verplicht is, Autoriteit Persoonsgegevens. Nr. 64418, 27 november 2019.
[97] Regeling Avg Defensie, Artikel 3 lid 3; Artikel 36 lid 3 Wpg; Artikel 39 lid lid Avg.
[98] WP29 richtlijn DPIA; WPG29 richtlijn voor FG's; Rijksmodel DPIA.
[99] Een verwerker verwerkt ten behoeve van een verwerkingsverantwoordelijke persoonsgegevens, zonder dat hij aan diens rechtstreekse gezag onderworpen is.

Bij nationale inzet op basis van bijstand of Militaire Steunverlening in het Openbaar Belang (MSOB) wordt de krijgsmacht ingezet onder aansturing en verantwoordelijkheid van civiel gezag, zoals de officier van justitie of de burgemeester. De krijgsmacht oefent daarbij taken en bevoegdheden uit van het ondersteunde civiele gezag. De krijgsmacht heeft daarbij geen eigen bevoegdheden. Er mogen in dat geval alleen bevoegdheden uitgeoefend worden van het ondersteunde civiele gezag. De uitoefening van die bevoegdheden vindt plaats onder aansturing en verantwoordelijkheid van dat civiele gezag. Als de MB/MSOB (mede) bestaat uit het verwerken van persoonsgegevens, dan moeten verwerkersafspraken opgesteld worden. Daarnaast moet er speciale aandacht zijn voor de inrichting van de aansturing en het toezicht door het civiele gezag op de verwerking van persoonsgegevens, om te voorkomen dat er feitelijk sprake is van aansturing en daarmee verwerkingsverantwoordelijkheid bij Defensie. Indien het gaat om het toepassen van bevoegdheden vallend onder de Wpg is dit alleen toegestaan indien defensiemedewerkers daarvoor zijn geautoriseerd door de Wpg-beheerder[100]. In dit laatste geval is Defensie wel verwerkersverantwoordelijke.

4.2.1.4 Rechtstreeks gezag

Er is alleen sprake van een verwerkersrelatie als de verwerker niet aan het rechtstreeks gezag van de verwerkingsverantwoordelijke is onderworpen. Wanneer iemand ondergeschikt is aan de verwerkingsverantwoordelijke of er anderszins sprake is van een hiërarchische verhouding (bijvoorbeeld medewerker, gedetacheerd bij de verwerkingsverantwoordelijke of een ZZP'er die werkt onder de instructies van een opdrachtgever), dan is er geen sprake van een verwerkersrelatie.
Wanneer individuele medewerkers worden ingehuurd of gedetacheerd, kunnen er twee situaties ontstaan: de medewerker werkt volledig 'op kantoor' en gedraagt zich feitelijk als een gewone werknemer. In dit geval is er geen verwerkersovereenkomst nodig (hoewel er wel afspraken worden gemaakt over bijvoorbeeld geheimhouding). Of de medewerker bepaalt grotendeels zelf de invulling van de werkzaamheden waardoor er geen gezagsverhouding is. Een verwerkersovereenkomst (of –afspraken) is dan wel nodig.
Indien een medewerker gedetacheerd is bij een verwerkersverantwoordelijke t.b.v. het uitvoeren van een taak/bepaalde werkzaamheden, maar voor de uitvoering van die taak gebruik maakt van middelen (bijvoorbeeld IT-infrastructuur) van de eigen organisatie dienen hiervoor wel verwerkersafspraken te worden opgesteld.

[100] Zie bijlage B en paragraaf 4.4.2., alsmede artikel 6 Wpg

Bijlage B Checklist social media monitoring

Stem altijd af met uw Avg-coördinator of Wpg-Privacyfunctionaris en JZ. Gebruik de hyperlinks in de checklist voor nadere informatie. De checklist is opgesteld ten behoeve van verwerkingen vallend binnen de reikwijdte van de Avg. Een deel van de punten van de checklist is daardoor niet van toepassing op het verwerken van politiegegevens.

	**1. Heeft u een gerechtvaardigd doel?** Een welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doel *is nodig om een tool* in te zetten als middel om dat doel te bereiken. De doeleinden dienen uit de taakstelling van Defensie of wet- en regelgeving herleidbaar te zijn. *De doelomschrijving moet tijdens het verzamelproces een kader bieden waaraan getoetst kan worden of de gegevens wel of niet nodig zijn voor dat doel.*
	**2. Is de verwerking doeltreffend?** Weeg en onderbouw of het doel van de verwerking in verhouding staat tot de inbreuk op de privacy van betrokkenen. De voorgestelde inbreuk dient niet verder te gaan dan noodzakelijk (proportionaliteit) en er dienen geen minder ingrijpende middelen voorhanden te zijn om hetzelfde resultaat te bereiken (subsidiariteit). *Waarom kan het doel niet op een andere, minder ingrijpende, manier worden bereikt? Onderbouw de inbreuk op de privacy van betrokkenen.*
	**3. Heeft u een wettelijke grondslag?** Is er een wettelijke verplichting, een taak van algemeen belang, een taak in het kader van de uitoefening van het openbaar gezag of een gerechtvaardigd belang? De grondslag dient concreet onderbouwd te zijn. *De algemene juridisch kaders voor activiteiten van de krijgsmacht in de informatieomgeving geven de mogelijke wettelijke grondslagen aan. Stem altijd af met uw Avg-coördinator of Wpg-Privacyfunctionaris en JZ.*
	**4. Heeft u een gerechtvaardigd belang?** Gerechtvaardigd belang kan niet gebruikt worden door overheidsinstanties in het kader van de uitoefening van hun taken. Wel zijn er mogelijkheden voor de toepassing van deze grondslag in het kader van behoorlijke beheer en de werking van overheidsinstanties ('typisch bedrijfsmatige handelingen"). Om deze grondslag te gebruiken moet er een duidelijke belangenafweging plaatvinden. *ICT- en computersystemen goed beveiligen en beschermen kan een gerechtvaardigd belang zijn. Wat niet als een gerechtvaardigd belang kwalificeert, is een algemeen belang van 'de samenleving'.*

	**5. Staat uw verwerking in het register van verwerkingsactiviteiten?** Alle verwerking die vallen onder de Avg, de Wpg en de RGMO moeten in registers zijn opgenomen. Zorg dat de registratie van de verwerking wordt vastgesteld. *Zorg dat de DPIA en verwerkersovereenkomst worden opgenomen in het register.*
	**6. Is Defensie de verwerker?** Wordt de taak uitgevoerd door Defensie voor een andere partij (verwerkingsverantwoordelijke)? Controleer of de andere partij beschikt over de benodigde wettelijke grondslag en bevoegdheden. Zorg tevens dat de inrichting van de aansturing en het toezicht is afgestemd om te voorkomen dat er feitelijk sprake is van aansturing door Defensie (en daarmee ook verwerkings-verantwoordelijkheid waarvoor een zelfstandig rechtsgrond nodig is). Zorg dat verwerkersafspraken worden vastgelegd.
	**7. Heeft u een DPIA opgesteld?** Een DPIA dient door of namens de verwerkingsverantwoordelijke vastgesteld te worden. Het opstellen wordt namens de Avg-beheerder of Wpg-beheerder gedaan, bij voorkeur in een multidisciplinair team, voordat de verwerking kan plaatsvinden. *Tip: besteed bijzondere aandacht aan de risicoafweging (onderdeel C rijksmodel DPIA). Bepaal of de risico's voor de rechten en vrijheden van natuurlijke personen kunnen worden afgedekt door mitigerende maatregelen.*
	**8. Past de tool bij het doel van de verwerking en is gebruik proportioneel en subsidiair?** Zorg voor *voorwaarden en waarborgen* zodat een tool alleen gebruikt wordt waarvoor deze bedoeld is en alleen met de reikwijdte waarvoor deze bedoeld is (begrenzing gebruik). Zorg dat bekend is welke bron(nen) de tool ontsluit en of dit in overeenstemming is met de gebruikers-voorwaarden en de privacyverklaring(en) van deze bron(nen). Zorg dat bekend is hoe de tool werkt (borging juistheid, integriteit, actualiteit en beveiliging) en hoe lang persoonsgegevens of naar personen herleidbare gegevens bewaard worden. *Tip: Zorg dat de analyse van de gebruikersvoorwaarden aantoonbaar is.*
	**9. Is het advies van de FG op de DPIA verwerkt?** Een DPIA dient aan de FG voorgelegd te worden ter advies. Neem in het rapport op wat de FG heeft geadviseerd en licht toe wat met het advies is gedaan. *Tip: zorg in een vroeg stadium voor afstemming over het doel en grondslag.*

	**10. Doet Defensie een beroep op een verwerker?** Zorg ervoor dat een verwerkersovereenkomst opgesteld wordt. Borg dat de overeengekomen maatregelen met de verwerker worden bewaakt en nageleefd. *Is in de overeenkomst overeengekomen dat de verwerker rapportages oplevert over de naleving van de gegevensbeschermingsmaatregelen? Zorg dat in de organisatie de verantwoordelijkheden belegd zijn voor de bewaking van de realisatie hiervan.*
	**11. Is de verwerking transparant?** De overheid dient open en transparant te zijn. Dat geldt ook voor Defensie. Communiceer over de verwerking van persoonsgegevens, zorg waar nodig voor informatievoorziening aan betrokkenen over welke data voor welk doel (verder)verwerkt worden en neem dit op in de privacyverklaring.

Bijlage C Afkortingen en begrippen

C.1 Afkortingen

AIVD: Algemene Inlichtingen- en Veiligheidsdienst
AP: Autoriteit Persoonsgegevens
Avg: Algemene verordening gegevensbescherming
BA: Beveiligingsautoriteit
BOA: Buitengewone opsporingsambtenaar
BS: Bestuursstaf
CDS: Commandant der Strijdkrachten
CLAS: Commando Landstrijdkrachten
CLSK: Commando Luchtstrijdkrachten
CTIVD: Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten
CZSK: Joint Informatievoorziening Commando
DOPS: Directie Operaties
DMO: Defensie Materieel Organisatie
DOSCO: Defensie Ondersteuningscommando
DPIA: Data Protection Impact Assessment
ECLI: European Case Law Identifier
EDBP: European Data Protection Board
EHRM: Europees Hof voor de Rechten van de Mens
EVRM: Europees Verdrag voor de Rechten van de Mens
FG: Functionaris Gegevensbescherming
GEB: Gegevensbeschermingseffectbeoordeling
HvJ: Hof van Justitie
JIVC: Joint Informatievoorziening Commando
KMar: Koninklijke Marechaussee
LIMC: Land Information Manoeuvre Centre
MB: Militaire Bijstand
MIVD: Militaire inlichtingen en Veiligheidsdienst
MSOB: Militaire Steunverlening in het Openbaar Belang
OSINT: Open source intelligence tools
RGMO: Regeling Gegevensbescherming Militaire Operaties
SA: Situational Awareness
SU: Situational Understanding
UAvg: Uitvoeringswet Avg
Wbp: Wet bescherming persoonsgegevens
Wiv: Wet op de inlichtingen en veiligheidsdiensten
Wjsg: Wet justitiële en strafvorderlijke gegevens
WP: Working Party
Wpg: Wet politiegegevens

C.2 Begrippenkader

Begrippen	Toelichting
Autoriteit Persoonsgegevens	Toezichthouder op de Avg, de UAvg en de Wpg.
Avg	Verordening (EU) 2016/679 van het Europees parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. In de Avg zijn de belangrijkste regels voor de omgang met persoonsgegevens in Nederland vastgelegd.
Avg-beheerder	Het diensthoofd die namens de minister van Defensie belast is met de zorg voor de naleving van de Avg en de wet ten aanzien van verwerkingen die gevoerd worden binnen het dienstonderdeel. Als zogenoemde Avg-beheerder zijn de operationele commandanten van de krijgsmachtonderdelen, de commandant Defensie Ondersteuningscommando, de directeur van de Defensie Materieel Organisatie en de plaatsvervangend secretaris-generaal voor de Bestuursstaf aangewezen.
Avg-coördinator	Functionaris, aangewezen door de Avg-beheerder, die de uitvoering van de AVG en de wet, en de feitelijke handelingen die daarvoor nodig zijn, binnen het betreffende dienstonderdeel coördineert.
GEB / DPIA	Een beoordeling van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.
Metadata	Metadata zijn gegevens die de karakteristieken van bepaalde gegevens beschrijven – dus data over data. Voorbeelden van metadata zijn: welke browser of telefoon iemand gebruikt, datum opstellen document en de geschreven taal van een tekst.
Persoonsgegeven	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Pseudonimisering	Het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder dat er aanvullende gegevens worden gebruikt, mits deze aanvullende gegevens apart worden bewaard en technische en organisatorische maatregelen worden genomen om ervoor te zorgen dat de persoonsgegevens niet aan een geïdentificeerde of identificeerbare natuurlijke persoon worden gekoppeld.
Politiegegeven	Een politiegegeven is elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, met uitzondering van: • de uitvoering van wettelijke voorschriften anders dan de Wet administratiefrechtelijke handhaving verkeersvoorschriften; • de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, bedoeld in artikel 1, eerste lid, onderdeel i, onder 1° en artikel 4, eerste lid, onderdeel f, van de Politiewet 2012.

Register van verwerkingsactiviteiten	Register waarin alle geheel of gedeeltelijk geautomatiseerde verwerkingen van persoonsgegevens worden bijgehouden. Met dit centrale register wordt inzichtelijk en overzichtelijk weergegeven welke processen en activiteiten er met persoonsgegevens plaatsvinden inclusief de verwerkingsdoelen en wettelijke grondslagen. Ook wordt vastgelegd op welke wijze en hoe lang de gegevens worden bewaard, aan wie ze worden verstrekt en hoe de beveiliging op hoofdlijnen geregeld is.
Scraping tools	Software / *tools* gericht op het verzamelen (scrapen) van (persoons)gegevens van publiek toegankelijke bronnen, waaronder *social media.*
Social media	Een verzamelnaam voor allerlei internettoepassingen die interactie in zowel tekst als beeld tussen de gebruikers mogelijk maken, zoals *webblogs*, microblogs (zoals Twitter), fora, videosites en sociale netwerken (zoals Facebook).
Social media monitoring	Het bijhouden en analyseren van uitingen in de *social media*. Dit kan voor verschillende doeleinden worden toegepast zoals het snel op vragen en kritiek vanuit de samenleving/consumenten te kunnen reageren, het analyseren van trends (bijv. of men positief of negatief spreekt over een organisatie), voor het monitoren van evenementen ten behoeve van de veiligheid en beveiliging of *situational awareness*.
Social media monitoring tools	Software met bijvoorbeeld zoek- en netwerkanalysefuncties, waarbij *social media* sites gelijktijdig kunnen worden bevraagd. Bijvoorbeeld *webbased* applicaties, die gericht (persoons)gegevens verzamelen van *social media* op basis van bepaalde *keywords*, zoals een bepaalde bedrijfstak, een dienst, een incident, een persoon of een evenement.
Uitvoeringswet Avg	De Avg is rechtstreeks van toepassing in Nederland. Daar waar de Avg ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAvg).
Verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/ dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
Verwerking van persoonsgegevens	Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.
Verwerken van politiegegevens	Elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens.
Verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
Wet politiegegevens	De Wpg regelt de verwerking van politiegegevens door de Nationale Politie, de bijzondere opsporingsdiensten, de Koninklijke marechaussee en de Rijksrecherche.
Wpg-beheerder	De Wpg-beheerder draagt zorg voor naleving van de regelgeving omtrent verwerking van politiegegevens door

	de Koninklijke Marechaussee. De Commandant Koninklijke Marechaussee is Wpg-beheerder. Hij doet dit namens de minister van Defensie.