Ontwerp	Besluit gegevensverwerking Defensie
Datum	3 juli 2026
Status	Voor internetconsultatie

Besluit van [datum], houdende regels over het verwerken van persoonsgegevens voor de gereedstelling en inzet van de krijgsmacht (Besluit gegevensverwerking Defensie)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Defensie van [datum], nr….;

Gelet op de artikelen 4.2, vierde lid, 4.7, derde lid, 4.8, derde lid, 4.9, achtste lid, en 4.13, vierde lid, van de Wet op de defensiegereedheid en artikel 3, vierde lid, van de Uitvoeringswet Algemene verordening gegevensbescherming;

De Afdeling advisering van de Raad van State gehoord (advies van [datum], nr. ...);

Gezien het nader rapport van Onze Minister van Defensie van [datum], nr. ...;

Hebben goedgevonden en verstaan:

HOOFDSTUK 1. Algemene bepalingen

Artikel 1.1 (begripsbepalingen)

In dit besluit wordt verstaan onder:

artificiële intelligentie-systeem: een op een machine gebaseerd systeem dat is ontworpen om met verschillende niveaus van autonomie te werken en dat na het inzetten ervan aanpassingsvermogen kan vertonen, en dat, voor expliciete of impliciete doelstellingen, uit de ontvangen input afleidt hoe output te genereren zoals voorspellingen, inhoud, aanbevelingen of beslissingen die van invloed kunnen zijn op fysieke of virtuele omgevingen;

wet: Wet op de defensiegereedheid.

HOOFDSTUK 2. GEREEDSTELLING

§ 2.1 Algemene bepalingen

Artikel 2.1 (voorwaarden gegevensverwerking)

1. Onze Minister voorziet voor de verwerking van persoonsgegevens bij of krachtens de wet in functiescheiding, waardoor bij de uitvoering van de in artikel 2.1, tweede lid, van de wet bedoelde activiteiten onderscheid wordt gemaakt in verschillende taken en rollen.

2. Het verwerken van persoonsgegevens op grond van de artikelen 4.9 tot en met 4.12 van de wet en de artikelen 2.4, tweede lid, en 2.6, eerste en tweede lid, van dit besluit, en de toegang tot die gegevens geschiedt slechts door de daartoe gemachtigde functionarissen.

3. De machtiging bevat een omschrijving van de verwerkingen en bronnen waartoe de functionaris wordt gemachtigd en de onderdelen van de taak ter uitvoering waarvan de verwerkingen worden gedaan.

4. Onze Minister zorgt ervoor dat de gemachtigde functionarissen voor zover relevant voor hun functie:

a. bekend zijn met het informatieproces binnen de defensieonderdelen, in het bijzonder de verschillende vormen van verwerkingen van persoonsgegevens op grond van de wet;

b. weten wanneer en hoe zij persoonsgegevens mogen verwerken op grond van de relevante wet- en regelgeving; en

c. bewust zijn van de risico’s met betrekking tot de verwerking van persoonsgegevens.

Artikel 2.2 (logging gegevensverwerking)

1. Onze Minister legt langs elektronische weg vast door wie en wanneer persoonsgegevens ten behoeve van persoonsgerichte kennisvergaring, bedoeld in artikel 4.9, vierde en vijfde lid, van de wet, in een geautomatiseerd systeem worden aangelegd, gewijzigd, geraadpleegd, verwijderd of verstrekt.

2. De vastgelegde gegevens, bedoeld in het eerste lid, worden uitsluitend gebruikt voor de controle van de rechtmatigheid van de gegevensverwerking, voor interne controles, ter waarborging van de integriteit en de beveiliging van persoonsgegevens.

Artikel 2.3 (verlenging bewaartermijn)

1. De Commandant der Strijdkrachten kan Onze Minister verzoeken om de bewaartermijn van persoonsgegevens, bedoeld in artikel 4.7, eerste lid, van de wet, met ten hoogste twee jaar te verlengen.

2. Een verzoek om verlenging van de bewaartermijn bevat in ieder geval:

a. een beschrijving van de gegevensverzameling waarin zich de persoonsgegevens bevinden dan wel, voor zover van toepassing, delen daarvan;

b. een aanduiding of het bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard als bedoeld in artikel 4.5 van de wet betreft;

c. een beschrijving van het doel waarvoor de persoonsgegevens zijn verwerkt en de specifieke activiteit in het kader waarvan de persoonsgegevens zijn verzameld;

d. de periode gedurende welke de persoonsgegevens al zijn bewaard;

e. de reden waarom verlenging van de bewaartermijn voor gebruik van de persoonsgegevens noodzakelijk, proportioneel en subsidiair is;

f. het gebruik van de persoonsgegevens in de afgelopen periode.

3. Onze Minister beoordeelt bij het verzoek of het verlengen van de bewaartermijn noodzakelijk is voor het verzekeren van de gereedheid van het militair vermogen van de krijgsmacht.

4. Indien het verzoek om verlenging van de bewaartermijn persoonsgegevens betreft die op grond van artikel 4.9, vierde en vijfde lid, van de wet zijn verwerkt, dan betrekt Onze Minister bij de beoordeling van het verzoek, bedoeld in het derde lid:

a. het verwachte optreden van de krijgsmacht in de relevante operationele omgeving;

b. de aard van het verwachte optreden van de krijgsmacht;

c. de mate van dreiging van de specifieke personen voor de veiligheid van de krijgsmacht of de militaire taakuitoefening van de betrokken eenheden;

d. of het focusgebied, bedoeld in artikel 4.9, vierde lid, van de wet, nog is aangewezen en de waarschijnlijkheid van verlenging;

e. of de categorieën van personen, bedoeld in artikel 4.9, vierde lid, onderdelen a tot en met c, van de wet, nog relevant zijn voor de desbetreffende doelen;

f. de waarschijnlijkheid dat de persoonsgegevens opnieuw verzameld zouden worden voor het doel.

§ 2.2 Gereedstellingsactiviteiten

Artikel 2.4 (opleiden, trainen en oefenen)

1. Ten behoeve van het opleiden, trainen en oefenen van defensiepersoneel, bedoeld in artikel 4.8, eerste lid, van de wet, worden opleidings- en trainingsprogramma’s en oefenomgevingen ontwikkeld die de operationele omgeving zo realistisch mogelijk benaderen.

2. Voor het ontwikkelen van deze opleidings- en trainingsprogramma’s en oefenomgevingen kunnen persoonsgegevens worden verwerkt.

3. Voor ingebruikname van het opleidings- of trainingsprogramma of de oefenomgeving worden, rekening houdend met de beschikbare technologie en de uitvoeringskosten, redelijke maatregelen getroffen om de persoonsgegevens in het programma of de omgeving te verwijderen, anonimiseren of pseudonimiseren.

4. Voor de activiteiten in artikel 4.8, eerste lid, onderdelen b tot en met e, van de wet, vindt de opleiding en training met persoonsgegevens uitsluitend plaats indien:

a. de persoon die de opleiding of training volgt, beschikt over theoretische kennis over het verwerken van persoonsgegevens; en

b. de opleiding en training geschiedt onder de verantwoordelijkheid en onder toezicht van een persoon die beschikt over voldoende deskundigheid over het verwerken van persoonsgegevens.

Artikel 2.5 (gebruik van materieel en technische hulpmiddelen)

1. Voor het opleiden, trainen en oefenen in de operationele oefenomgeving met en het onderhouden van materieel kunnen persoonsgegevens verwerkt worden, indien noodzakelijk voor het gebruik van het materieel. Na het gebruik van het materieel worden persoonsgegevens niet verder verwerkt, tenzij de persoonsgegevens ten minste zijn geanonimiseerd.

2. Het opleiden, trainen en oefenen in het gebruik van technische hulpmiddelen om de omgeving waar te nemen of om veilig en effectief gebruik te maken van het elektromagnetisch spectrum en het manipuleren en verstoren van de elektromagnetische straling in dat spectrum, vindt in beginsel op of boven militaire objecten plaats.

3. Op andere plaatsen dan op of boven militaire objecten is het gebruik van de technische hulpmiddelen gericht op de personen die deelnemen aan de specifieke activiteit van de opleiding, training of oefening. Indien gegevens zijn verzameld van andere personen dan de deelnemers aan de specifieke activiteit van de opleiding, training of oefening en waarbij redelijkerwijs voorzienbaar is dat deze persoonsgegevens een min of meer volledig beeld van bepaalde aspecten van iemands privéleven geven, dan worden deze persoonsgegevens onverwijld verwijderd.

Artikel 2.6 (ontwerpen, ontwikkelen en experimenteren)

1. Bij het ontwerpen en ontwikkelen van en het experimenteren met materieel, technologieën en technieken, bedoeld in artikel 4.8, eerste lid, onderdeel f, van de wet, kunnen persoonsgegevens worden gebruikt voor zover alle redelijke maatregelen zijn getroffen om persoonsgegevens ten minste te pseudonimiseren.

2. In afwijking van het eerste lid, kunnen ten behoeve van het trainen, valideren en testen van een artificiële intelligentie-systeem gegevensverzamelingen worden gebruikt. Die gegevensverzamelingen zijn zoveel mogelijk foutenvrij, relevant, voldoende representatief en volledig gericht op het veilig en beoogd gebruik van het artificiële intelligentie-systeem. Voor ingebruikname van een artificiële intelligentie-systeem worden alle redelijke maatregelen getroffen om de voor het trainen, testen of valideren verwerkte persoonsgegevens te verwijderen of anonimiseren.

3. Het gebruik van artificiële intelligentie-systemen, en de ontwikkeling daarvan gericht op dit gebruik, vindt plaats:

a. op een rechtmatige wijze;

b. op een zorgvuldige wijze, waarbij de menselijke gebruiker verantwoordelijk is voor de uitkomsten;

c. op een wijze die begrijpelijk en transparant is;

d. voor welbepaalde en uitdrukkelijk omschreven doeleinden en op een betrouwbare wijze;

e. op een controleerbare en beheersbare wijze, die menselijke controle en toezicht toelaat;

f. op een wijze die bij de toepassing ervan vooringenomenheid zoveel mogelijk beperkt.

§ 2.3 Informatiepositie

Artikel 2.7 (persoonsgerichte kennisvergaring op aanwijzing)

1. Onze Minister geeft een aanwijzing voor de persoonsgerichte kennisvergaring, bedoeld in artikel 4.9, vierde lid, van de wet.

2. Een aanwijzing bevat in ieder geval een beschrijving van:

a. de aanleiding om kennis te vergaren over de relevante operationele omgeving, waaronder een duiding van de dreigingen die er zijn voor het Koninkrijk of een bondgenoot en het kader waarin het optreden van de krijgsmacht mogelijk zal plaatsvinden;

b. het focusgebied binnen de relevante operationele omgeving;

c. het doel en de noodzaak van het vergaren van kennis over specifieke personen;

d. de categorieën van personen, bedoeld in artikel 4.9, vierde lid, onderdelen a tot en met c, van de wet, waarover kennis vergaard zal worden;

e. de militaire eenheid die bevoegd is om kennis te vergaren over specifieke personen.

3. Onze Minister geeft een aanwijzing als deze van oordeel is dat de persoonsgerichte kennisvergaring noodzakelijk is voor een veilig en doeltreffend optreden van eenheden of onderdelen van de krijgsmacht in de relevante operationele omgeving.

4. Een aanwijzing kan voor maximaal een jaar worden gegeven, en steeds verlengd worden voor ten hoogste een jaar.

5. In aanvulling op het tweede lid, bevat de verlenging van de aanwijzing een beschrijving van de noodzaak van die verlenging, van de afstemming met de Militaire Inlichtingen- en Veiligheidsdienst over de persoonsgerichte kennisvergaring en, in voorkomend geval, of een andere militaire eenheid de bevoegdheid dient te verkrijgen.

Artikel 2.8 (persoonsgerichte kennisvergaring door de commandant)

1. De commandant, die het bevel voert over een militaire eenheid, is bevoegd om op eigen initiatief gebruik te maken van de bevoegdheid, bedoeld in artikel 4.9, vierde en vijfde lid, van de wet, indien spoedeisende en gewichtige redenen dit vereisen om een veilig en doeltreffend optreden van de eenheid of het onderdeel in de relevante operationele omgeving te waarborgen.

2. Nadat de commandant de bevoegdheid om persoonsgericht kennis te vergaren op eigen initiatief heeft gebruikt wordt Onze Minister onverwijld om goedkeuring verzocht. Een verzoek om goedkeuring bevat in ieder geval een beschrijving van:

a. de personen waarover kennis wordt vergaard;

b. de aanleiding om kennis te vergaren over deze personen, waaronder een duiding van de dreigingen die er zijn voor het Koninkrijk of een bondgenoot en het kader waarin de kennis wordt vergaard;

c. het gebied waar binnen de relevante operationele omgeving gegevens over specifieke personen wordt vergaard;

d. het doel en de noodzaak, waaronder de dringende en gewichtige redenen voor het eigen initiatief, van het vergaren van kennis over specifieke personen;

e. de militaire eenheid die gebruikt heeft gemaakt van de bevoegdheid om kennis te vergaren over specifieke personen;

f. de verwachte duur van de kennisvergaring.

3. Indien Onze Minister bij de beoordeling van het verzoek tot het oordeel komt dat spoedeisende en gewichtige redenen de persoonsgerichte kennisvergaring vereisen, geeft deze goedkeuring voor het gebruik van de bevoegdheid en de voortzetting daarvan voor ten hoogste dertig dagen.

4. Indien voortzetting van de persoonsgerichte kennisvergaring noodzakelijk is na de termijn waarvoor goedkeuring is gegeven als bedoeld in het derde lid dan dient daartoe een aanwijzing, met inachtneming van artikel 2.7, te worden gegeven.

5. Bij het onthouden van de goedkeuring, bedoeld in het derde lid, wordt de verwerking van persoonsgegevens onmiddellijk gestaakt. Onze Minister bepaalt welke gevolgen verbonden dienen te worden aan de verzamelde persoonsgegevens.

Artikel 2.9 (afstemming MIVD persoonsgerichte kennisvergaring)

1. De Militaire Inlichtingen- en Veiligheidsdienst wordt onverwijld in kennis gesteld over de persoonsgerichte kennisvergaring die betrekking heeft op personen als bedoeld in artikel 4.9, vierde lid, onderdeel a, van de wet.

2. De Commandant der Strijdkrachten en het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst plegen overleg over in de kennisgeving benoemde activiteiten.

3. Op basis van de kennisgeving, bedoeld in het eerste lid, kan het hoofd van de Militaire Inlichtingen- en Veiligheidsdienst advies geven aan Onze Minister over het wijzigen of intrekken van de aanwijzing, bedoeld in artikel 2.7, of het onthouden van de goedkeuring, bedoeld in artikel 2.8.

4. Gegevens verwerkt ten behoeve van de persoonsgerichte kennisvergaring, bedoeld in artikel 4.9, vierde en vijfde lid, van de wet, en ontvangen van een dienst worden uitsluitend verstrekt aan personen of instanties als bedoeld in artikel 4.13 van de wet, indien de betrokken dienst daartoe toestemming heeft verleend.

§ 2.4 Gegevensverstrekking

Artikel 2.10 (gegevensverstrekking aan personen en instanties)

Gegevens, waaronder persoonsgegevens, die worden verwerkt overeenkomstig de artikelen 4.9 tot en met 4.12 van de wet, kunnen, voor zover zij deze behoeven voor een goede uitvoering van hun taak, worden verstrekt aan:

a. de deelnemers van het samenwerkingsverband, bedoeld in artikel 2, derde lid, van de Regeling organisatie Kustwacht Nederland, en de Directeur Kustwacht, bedoeld in artikel 14 van die regeling, ten behoeve van de taakuitvoering in de Kustwacht;

b. de Kustwacht voor Aruba, Curaçao en Sint Maarten alsmede voor de openbare lichamen Bonaire, Sint Eustatius en Saba, bedoeld in artikel 2, eerste lid, van de Rijkswet Kustwacht voor Aruba, Curaçao en Sint Maarten alsmede voor de openbare lichamen Bonaire, Sint Eustatius en Saba, ten behoeve van de taken, bedoeld in artikel 2, tweede tot en met vierde lid, van die wet.

HOOFDSTUK 3. INZET EN TERBESCHIKKINGSTELLING VAN DE KRIJGSMACHT

Artikel 3.1 (toepassingsbereik)

1. Dit hoofdstuk is van toepassing op de verwerking van persoonsgegevens bij de inzet of het ter beschikking stellen van de krijgsmacht ter uitvoering van de in artikel 97 van de Grondwet omschreven taken.

2. De krijgsmacht kan persoonsgegevens verwerken omtrent de voor een veilige en doeltreffende inzet van de krijgsmacht relevante operationele omgeving en voor zover dit noodzakelijk is voor de uitoefening van het internationale of nationale mandaat voor de inzet.

Artikel 3.2 (verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard)

1. Biometrische en genetische gegevens mogen uitsluitend verwerkt worden voor het vaststellen en de verificatie van de identiteit van een persoon.

2. De verwerking van genetische gegevens vindt alleen plaats ten aanzien van personen die verdacht worden van strafbare feiten die ofwel verband houden met een gewapend conflict ofwel gericht zijn tegen de veiligheid van de troepenmacht.

3. Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakbond blijkt, en de verwerking van gegevens over gezondheid, seksuele leven en seksuele gerichtheid, alsmede persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen, worden niet verwerkt, tenzij:

a. dat voor het doel van de gegevensverwerking noodzakelijk is;

b. deze persoonsgegevens in aanvulling zijn op de verwerking van andere persoonsgegevens betreffende de persoon; en

c. de gegevens afdoende zijn beveiligd, waaronder in voorkomend geval de versleuteling van deze gegevens en het beperken van toegang tot deze gegevens.

Artikel 3.3 (gegevensverstrekking)

1. Het verstrekken van gegevens, waaronder persoonsgegevens, verwerkt in het kader van inzet van de krijgsmacht, aan de politie, de Koninklijke marechaussee en het openbaar ministerie, voor zover zij deze behoeven voor de goede uitvoering van hun wettelijke taken in verband met het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten, is toegestaan voor zover de vertrouwelijkheid zich daar niet tegen verzet.

2. Het verstrekken van persoonsgegevens als onderdeel van operationele inlichtingenproducten aan andere deelnemende landen of internationale organisaties binnen de bevelsstructuur van een operatie is toegestaan, voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 3.1.

3. Het verstrekken van persoonsgegevens anders dan genoemd in het tweede lid aan andere deelnemende landen of internationale organisaties die deelnemen aan dezelfde operatie is toegestaan, voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 3.1, en onder de

voorwaarde dat deze persoonsgegevens slechts kunnen worden verwerkt door de ontvanger voor het doel waarvoor ze zijn verstrekt en voor de duur van de betreffende operatie.

4. De verstrekking van persoonsgegevens aan derde landen of internationale organisaties blijft achterwege indien de verstrekking in het specifieke geval in strijd is met de belangen van het Koninkrijk of een gevaar oplevert voor het recht op leven, menselijke integriteit en vrijheid of andere fundamentele mensenrechten van de betrokkene.

Artikel 3.4 (bewaartermijn)

Indien persoonsgegevens niet langer noodzakelijk zijn voor het doel, bedoeld in artikel 3.1, worden deze verwijderd en vernietigd, tenzij wettelijke voorschriften over bewaring daaraan in de weg staan.

Artikel 3.5 (rechten van betrokkene)

1. Onze Minister maakt de volgende informatie publiekelijk kenbaar:

a. de contactgegevens van het Ministerie van Defensie inzake gegevensverwerking;

b. de contactgegevens van de functionaris voor gegevensbescherming;

c. de verwerkingsdoeleinden waarvoor persoonsgegevens verwerkt kunnen worden;

d. de rechten van de betrokkene, bedoeld in het tweede en derde lid;

e. het recht een klacht in te dienen bij de Autoriteit persoonsgegevens, en de contactgegevens van die autoriteit.

2. Onze Minister deelt een ieder op diens aanvraag zo spoedig mogelijk, doch uiterlijk binnen drie maanden mede of en, zo ja, welke hem betreffende persoonsgegevens voor het doel, bedoeld in artikel 3.1, zijn verwerkt.

3. Op het recht van kennisneming, bedoeld in het tweede lid, zijn de artikelen 4.15, tweede tot en met vijfde lid, 4.16 en 4.17 van de wet van overeenkomstige toepassing.

HOOFDSTUK 4. SLOTBEPALINGEN

Artikel 4.1 (inwerkingtreding)

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Artikel 4.2 (citeertitel)

Dit besluit wordt aangehaald als: Besluit gegevensverwerking Defensie

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

PM

NOTA VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Het onderhavige Besluit gegevensverwerking Defensie (hierna ook: het besluit) is de uitwerking bij algemene maatregel van bestuur van bepalingen van de Wet op de defensiegereedheid (hierna: Wodg). In dit Besluit wordt daarbij uitvoering gegeven aan de delegatiegrondslagen uit hoofdstuk 4 van de Wodg en artikel 3, vierde lid, Uitvoeringswet Algemene verordening gegevensbescherming (hierna: UAVG).[1] De delegatiegrondslagen opgenomen in hoofdstuk 3 van de Wodg over de fysieke leefomgeving zijn uitgewerkt in het Besluit defensiegereedheid fysieke leefomgeving. De delegatiegrondslagen over personele onderwerpen opgenomen in artikel 4a, tweede lid, van de Wet op de medische keuringen[2] en de artikelen 12hbis, vierde lid, en 12hter, vierde lid, van de Wet ambtenaren defensie[3] zijn uitgewerkt in het Besluit defensiegereedheid personeel.

In hoofdstuk 2 van dit besluit zijn in de eerste plaats de opdrachten tot het stellen van regels bij algemene maatregel van bestuur over gegevensverwerking bij de gereedstelling uitgewerkt. Het betreft:

a. regels over de procedure van het verlengen van de bewaartermijn (artikel 4.7, derde lid, Wodg); en

b. nadere regels over de gereedstellingsactiviteiten (artikel 4.8, derde lid, Wodg).

Ten tweede bevat hoofdstuk 2 van dit besluit een uitwerking van grondslagen die de mogelijkheid geven om nadere regels te stellen. Het betreft:

c. regels over de voorwaarden die aan de verwerking van persoonsgegevens kunnen worden gesteld (artikel 4.2, vierde lid, onderdeel a, Wodg);

d. nadere regels over de aanwijzing en goedkeuring van de persoonsgerichte kennisvergaring alsmede over de afstemming met de Militaire Inlichtingen- en Veiligheidsdienst (artikel 4.9, achtste lid, Wodg);

e. een aanwijzing van de Kustwacht Nederland en Kustwacht Caribisch Gebied als personen en instanties waaraan persoonsgegevens verstrekt mogen worden (artikel 4.13, vierde lid, Wodg).

In hoofdstuk 3 van dit besluit is de opdracht tot het stellen van regels bij algemene maatregel van bestuur over gegevensverwerking bij inzet uitgewerkt (artikel 3, vierde lid, UAVG).

---

[1] Wijziging in artikel 7.1 van de Wet op defensiegereedheid (Wodg).
[2] Wijziging in artikel 7.2 van de Wodg.
[3] Wijziging in artikel 7.3 van de Wodg.

2. Hoofdlijnen van het besluit

De regels in dit besluit moeten gelezen worden in de context van de Wet op de defensiegereedheid. Hieronder zal eerst ingegaan worden op de systematiek van de wet, met nadruk op hoofdstuk 4 daarvan voor de gereedstelling en artikel 7.1 voor inzet, waarna de hoofdlijnen van het besluit worden beschreven.

2.1 Systematiek van de wet inzake gereedstelling

Aanleiding

De aanleiding van de wet wordt gevormd door de toename in frequentie en intensiteit van conflicten in de buurt van Europa. De dreiging van een militair conflict waar Nederland bij betrokken kan raken is reëel.[4] De krijgsmacht heeft in dat verband als taak om het Koninkrijk te verdedigen alsmede het beschermen van de belangen van het Koninkrijk.[5] Dit omvat ook het verdedigingen van het grondgebied van onze bondgenoten, en om aanvallen te voorkomen.[6] Om Nederland en onze bondgenoten te kunnen verdedigen moet Defensie gereed staan. Op dit moment vereist dit het versterken en groeien van de krijgsmacht, waarbij ook meer oefeningen, logistiek en voorbereidende activiteiten uitgevoerd moeten kunnen worden. Daarbij loopt Defensie tegen allerlei wetten en regels aan, die regelmatig ontoereikend of niet uitvoerbaar zijn. Soms ontbreekt een grondslag om huidige activiteiten te kunnen uitvoeren, vaak op eigen defensieterreinen. Het ontbreken van grondslagen speelt vooral in de informatieomgeving.

Daadwerkelijke en stelselmatige gereedheid

Het hoofddoel van de Wodg is het verzekeren van een daadwerkelijke en stelselmatige gereedheid van het militair vermogen van de krijgsmacht in de operationele omgeving. In hoofdstuk 2 van de wet is neergelegd dat de verantwoordelijkheid, de zorg, voor de daadwerkelijke gereedstelling door de Minister van Defensie wordt gedragen. Deze publieke taak wordt op hoofdlijnen in hoofdstuk 2 vastgelegd en met betrekking tot de informatieomgeving in hoofdstuk 4 verder uitgewerkt.

Wettelijke grondslag voor het verwerken van persoonsgegevens

Hoofdstuk 4 van de wet voorziet in een wettelijke grondslag voor het verwerken van persoonsgegevens voor zover dit noodzakelijk is voor het verrichten van gereedstellingsactiviteiten die worden uitgevoerd door de krijgsmacht en de defensieonderdelen. In samenhang met de bevoegdheid om persoonsgegevens te verwerken bevat de wet ook diverse begrenzingen en waarborgen bij die gegevensverwerking. Daarmee wordt beoogd een balans te vinden tussen de noodzaak om persoonsgegevens te verwerken ten behoeve van de gereedstelling en het beschermen van de persoonlijke levenssfeer.

Artikel 4.2, eerste lid, van de wet bevat de grondslag voor het verwerken van persoonsgegevens voor zover dit noodzakelijk is voor de gereedstelling. In de paragrafen 4.2 tot en met 4.4 van de wet worden de omstandigheden wanneer persoonsgegevens verwerkt

---

[4] Militaire Inlichtingen- en Veiligheidsdienst, *Openbaar Jaarverslag 2025*, bijlage bij *Kamerstukken II* 2025/26, 29 924, nr. 295.
[5] Artikel 97, eerste lid, van de Grondwet.
[6] *Kamerstukken II* 1999/2000, 26 900, nrs. 1-2, p. 41 en *Kamerstukken II* 1996/97, 25 367 (R 1593), nr. 3.

mogen worden nader afgebakend en begrenzingen gesteld aan die verwerkingen. Het gaat daarbij om specifieke regels voor de verwerking van persoonsgegevens bij het verrichten van gereedstellingsactiviteiten, het verkrijgen van een informatiepositie voor de krijgsmacht en het bewaken en beveiligen van de netwerk- en informatiesystemen van de defensieonderdelen, militaire objecten en het defensiepersoneel.

Algemene waarborgen

In paragraaf 4.1 van de wet zijn de algemene voorwaarden en waarborgen opgenomen bij het verwerken van persoonsgegevens. Een belangrijke waarborg daarin is de gedeeltelijke van overeenkomstige toepassing verklaring van de Algemene verordening gegevensbescherming (AVG)[7] en UAVG op deze gegevensverwerkingen. Daarnaast gaat het bij de algemene waarborgen om een inspanningsverplichting om persoonsgegevens te anonimiseren of pseudonimiseren, een verplichting tot het treffen van passende en technische en organisatorische maatregelen en begrenzingen die gesteld worden aan het gebruik van bronnen. Voorts bevat de wet een algemene regel bij het verwerken van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard en voor het verwerken van omvangrijke gegevensverzamelingen voor alle verwerkingen op grond van de wet. Ten slotte voorziet de wet in een algemene bewaartermijn voor alle verwerkingen op grond van de wet.

Gegevensverstrekking

Artikel 4.13 van de wet voorziet in een specifiek regime voor het verstrekken van gegevens aan derden. Die gegevensverstrekking kan alleen plaatsvinden binnen de gronden of voorwaarden opgenomen in die bepaling. Daarbij gelden voor verstrekkingen aan het buitenland aanvullende waarborgen, zoals een vertrouwelijkheidsbeoordeling en belangenafweging.

Rechten van de betrokkene

Voor de rechten van betrokkene wordt in paragraaf 4.6 van de wet voorzien in een eigen regime, waarbij rekening wordt gehouden met de specifieke context waarin de gegevensverwerkingen in het kader van de gereedstelling plaatsvindt.

2.2 Systematiek van regels over gegevensverwerking bij inzet

Uit artikel 97, tweede lid, van de Grondwet volgt dat de regering het oppergezag heeft over de krijgsmacht. De regering draagt daarmee de verantwoordelijkheid voor de inzet of het ter beschikking stellen van de krijgsmacht. De bevoegdheid om de krijgsmacht in te zetten of ter beschikking te stellen is beperkt tot de taken opgenomen in het eerste lid van artikel 97 van de Grondwet: de verdediging en bescherming van de belangen van het Koninkrijk en de

[7] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119).

handhaving en de bevordering van de internationale rechtsorde.[8] Wanneer de regering besluit tot het inzetten van de krijgsmacht, dan geeft de krijgsmacht uitvoering aan een taak van algemeen belang.

Bij het uitvoeren van die taak van algemeen belang (de inzet ter uitvoering van artikel 97 van de Grondwet) kunnen, voor zover noodzakelijk voor de goede uitvoering daarvan persoonsgegevens verwerkt worden.[9] De AVG is in beginsel niet van toepassing op de verwerking van persoonsgegevens bij inzet of het ter beschikking stellen van de krijgsmacht. Met artikel 7.1 van de wet is artikel 3, derde lid, UAVG gewijzigd waarin de AVG en UAVG gedeeltelijk van overeenkomstige toepassing worden verklaard op de verwerking van persoonsgegevens bij inzet of het ter beschikking stellen van de krijgsmacht. In de UAVG wordt daarmee op wetsniveau verduidelijkt welke bepalingen van de AVG en UAVG van toepassing zijn. Bij het verwerken van persoonsgegevens bij gereedstelling en inzet van de krijgsmacht zijn dezelfde bepalingen uit de AVG en UAVG van overeenkomstige toepassing.[10] Daarnaast is in artikel 3, vierde lid, UAVG een expliciete delegatiegrondslag opgenomen om nadere regels te stellen in een algemene maatregel van bestuur, waarmee krachtens de wet beperkingen gesteld worden aan het recht op eerbiediging van de persoonlijke levenssfeer.

Met de wijziging van de UAVG is uitvoering gegeven aan het advies van de Afdeling advisering van de Raad van State op de Rijkswet betreffende goedkeuring van Conventie 108 en Conventie 108+.[11]

2.3 Het Besluit gegevensverwerking Defensie: één AMvB voor gegevensverwerking tijdens gereedstelling en inzet

In de Wodg zijn meerdere grondslagen opgenomen om de bepalingen over gegevensverwerking gedurende de gereedstelling uit te werken in een algemene maatregel van bestuur. Daarnaast wijzigt de Wodg ook artikel 3 UAVG op grond waarvan nadere regels gesteld kunnen worden over de gegevensverwerking tijdens de inzet of het ter beschikking stellen van de krijgsmacht ter uitvoering van de in artikel 97 van de Grondwet omschreven taken. In de voorbereiding van het besluit is besloten om zowel de regels over gegevensverwerking betreffende de gereedstelling als inzet op te nemen in één algemene maatregel van bestuur. Hiermee wordt benadrukt dat gereedstelling en inzet in elkaar overgaan en niet los van elkaar gezien kunnen worden.

Structuur van het besluit

---

[8] *Kamerstukken II* 1996/97, 25 367 (R 1593), nr. 3.
[9] Artikel 3, derde lid, onderdeel b, UAVG.
[10] Met uitzondering van de artikelen 9 en 10, hoofdstuk III en de artikelen 33, 34 en 36 van de AVG en de artikelen 22 tot en met 33 van de UAVG zijn de AVG en UAVG van overeenkomstige toepassing.
[11] Afdeling advisering van de Raad van State over de goedkeuring wijziging van verdrag over bescherming persoonsgegevens, *Kamerstukken II* 2023/24, 36 455 (R2188), nr. 4; Rijkswet houdende goedkeuring van het op 28 januari 1981 te Straatsburg tot stand gekomen Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Trb. 1988, 7); van het op 10 oktober 2018 te Straatsburg tot stand gekomen Protocol tot wijziging van het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Trb. 2018, 201 en Trb. 2023, 54), *Kamerstukken II* 2023/24, 36 455 (R2188), nr. 2.

Het Besluit gegevensverwerking Defensie volgt op hoofdlijnen de hoofdstukindeling van de Wodg en de chronologische volgorde waarin delegatiegrondslagen zijn opgenomen, waarmee de onderlinge samenhang wordt uitgedrukt.

Algemene bepalingen (hoofdstuk 1)

De wet werkt door in het besluit. Zo is het begrippenapparaat van artikel 1.1 van de wet in beginsel ook van toepassing op de bepalingen van hoofdstuk 2 van het besluit. De begripsbepaling van artikel 1.1 van het besluit bevat dan ook uitsluitend die begrippen die verduidelijking vragen waarvoor nog geen beschrijving is gegeven in de wet.

Gereedstelling van de krijgsmacht (hoofdstuk 2)

Dit hoofdstuk bevat de (nadere) regels over het verwerken van persoonsgegevens ten behoeve van de gereedstelling van de krijgsmacht.

Algemene bepalingen (paragraaf 2.1)

De eerste paragraaf bevat de bepalingen die in beginsel van toepassing kunnen zijn op alle verwerkingen. Het gaat daarbij om de voorwaarden die aan een verwerking worden gesteld, bestaande uit functiescheiding, machtiging, deskundigheidseisen en logging. Daarnaast bevat het een uitwerking van de procedure voor het verlengen van de bewaartermijn.

Gereedstellingsactiviteiten (paragraaf 2.2)

De tweede paragraaf ziet op de gegevensverwerking ten behoeve van gereedstellingsactiviteiten en bevat nadere regels voor een deel van de specifieke activiteiten opgenomen in artikel 4.8, eerste lid, Wodg. Daarbij wordt voorzien in basisregels voor het opleiden, trainen en oefenen en het ontwikkelen van opleidings- en trainingsprogramma’s en oefenomgeving. Daarnaast bevat het specifieke regels voor het gebruik van materieel als onderdeel van het opleiden, trainen en oefenen en het onderhouden daarvan alsmede het gebruik van technische hulpmiddelen en het elektromagnetisch spectrum. Ook bevat het specifieke regels voor het ontwerpen, ontwikkelen en experimenteren.

Informatiepositie (paragraaf 2.3)

De derde paragraaf voorziet in nadere regels over de persoonsgerichte kennisvergaring als onderdeel van de informatiepositie. Het gaat daarbij om een uitwerking van het proces rondom de aanwijzing van de Minister van Defensie voor de persoonsgerichte kennisvergaring en diens goedkeuring indien een commandant op eigen initiatief persoonsgericht kennis heeft vergaard. Daarnaast betreft het nadere regels over de afstemming tussen de krijgsmacht en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) inzake de gerichte kennisvergaring van personen die een gevaar vormen voor de veiligheid van de krijgsmacht of de militaire taakuitoefening van de betrokken eenheden.

Gegevensverstrekking (paragraaf 2.4)

In de vierde paragraaf zijn de personen en instanties aangewezen aan wie of waaraan met het oog op een zwaarwegend belang persoonsgegevens verstrekt kunnen worden. Op dit moment zijn daarin de Kustwacht Nederland en Kustwacht Caribisch Gebied aangewezen.

Inzet en terbeschikkingstelling van de krijgsmacht (hoofdstuk 3)

Dit hoofdstuk bevat de regels over het verwerken van persoonsgegevens ten behoeve van de inzet of het ter beschikking stellen van de krijgsmacht. Dit hoofdstuk bouwt grotendeels voort op de Regeling Gegevensbescherming Militaire Operaties (RGMO). Inhoudelijke wijzigingen komen voort uit het advies van de Afdeling advisering van de Raad van State op de Rijkswet betreffende goedkeuring van Conventie 108 en Conventie 108+ en voortschrijdend inzicht. Het betreft onder meer een uitbreiding van de regels tot inzet onder exclusief nationaal mandaat, regels over de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard en een regime voor de rechten van betrokkene.

Slotbepalingen (hoofdstuk 4)

Dit slothoofdstuk bevat praktische voorschriften inzake het moment van inwerkingtreding.

3. Verhouding tot hoger recht

Op grond van de Wodg en de UAVG in samenhang met artikel 97 van de Grondwet kunnen persoonsgegevens verwerkt worden zowel bij de gereedstelling als de inzet of het ter beschikking stellen van de krijgsmacht. Deze verwerkingen maken een inbreuk op het recht op eerbiediging van de persoonlijke levenssfeer, zoals dit volgt uit de Grondwet, het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, het Handvest van de grondrechten van de Europese Unie en de AVG. In de memorie van toelichting bij de Wodg is uitgebreid ingegaan op de verwerking van persoonsgegevens die op grond daarvan kunnen plaatsvinden bij de gereedstelling.[12] In de memorie van toelichting op de Wet bescherming persoonsgegevens en de UAVG is ingegaan op de verwerking van persoonsgegevens bij de inzet of het ter beschikking stellen van de krijgsmacht.[13] Aangezien dit besluit een uitwerking is van de wet, is een nadere uitwerking van de verhouding tot hoger recht in deze nota van toelichting niet nodig. Hieronder wordt wel nader ingegaan over hoe de bepalingen in dit besluit in het licht van het hoger recht zich tot het bepaalde in de Wodg verhouden.

In dit besluit is geen subdelegatie voorzien naar het niveau van de ministeriële regeling.[14] Op dit moment wordt niet de noodzaak gezien om meer administratieve en gedetailleerde (technische) regels te stellen.[15]

Het vereiste van gemachtigde personen heeft als doel om te zorgen dat een beperkte kring van personen voor een bepaald doel toegang heeft tot persoonsgegevens en die ook mag verwerken.[16] Hiermee wordt bijgedragen aan het waarborgen van de integriteit en vertrouwelijkheid van de persoonsgegevens en de gegevensverwerking.

In § 2.2 van dit besluit zijn de categorieën van verwerkingen van persoonsgegevens bij de gereedstellingsactiviteiten en de voorwaarden die daarbij gelden nader uitgewerkt. Hierbij wordt de gereedstellingssystematiek gevolgd die in beginsel invulling geeft aan de beginselen van proportionaliteit en subsidiariteit van de verwerking van persoonsgegevens bij de

---

[12] PM verwijzing naar kamerstuk
[13] *Kamerstukken II* 1997/98, 25 892, nr. 3, p. 72, en *Kamerstukken II* 2017/18, 34 851, nr. 3, p. 90-91.
[14] Zie de grondslag daartoe: Artikel 4.2, vierde lid, Wodg.
[15] PM verwijzing advies RvS en nader rapport.
[16] Artikel 2.1, tweede tot en met vierde lid.

gereedstellingsactiviteiten. Met de bepalingen in § 2.2 wordt nader invulling gegeven aan de balans tussen het publieke belang van de gereedheid om persoonsgegevens te kunnen verwerken en de proportionaliteit en subsidiariteit daarvan met betrekking tot de individuele belangen en grondrechten van burgers.

In § 2.3 van dit besluit zijn de procedurele waarborgen omtrent de persoonsgerichte kennisvergaring verder uitgewerkt. Met de aanwijzing van de Minister van Defensie en de goedkeuring moet gewaarborgd worden dat de mogelijk grote inbreuk op de persoonlijke levenssfeer beperkt blijft tot het strikt noodzakelijke. In dat verband dient de MIVD ook onverwijld in kennis gesteld te worden wanneer de krijgsmacht persoonsgerichte kennisvergaring nodig acht van personen waarover een ernstig vermoeden bestaat dat deze een gevaar vormen voor de veiligheid van de krijgsmacht of de militaire taakuitoefening van de betrokken eenheden. Naar aanleiding daarvan kan er afstemming plaatsvinden tussen de krijgsmacht en de MIVD met het oog op, onder andere, het zoveel mogelijk voorkomen van een dubbele inbreuk op de persoonlijke levenssfeer.

De verstrekking van persoonsgegevens aan de Kustwacht Nederland en de Kustwacht voor Aruba, Curaçao en Sint Maarten alsmede voor de openbare lichamen Bonaire, Sint Eustatius en Saba (Kustwacht Caribisch Gebied) is een aanvulling op artikel 4.13 van de wet.[17] Met die verstrekking wordt het zwaarwegend belang van de openbare veiligheid en het voorkomen van wanordelijkheden en strafbare feiten gediend.[18] Het verstrekken van die gegevens draagt bij aan het versterken van de maritieme veiligheid op het water en de handelingsperspectieven binnen de rechtshandhavingsketen, doordat daarmee het omgevingsbeeld van de Kustwacht wordt verbeterd alsmede wordt zij in staat gesteld waar mogelijk handhavend op te treden. In het bijzonder kan daarbij worden gedacht aan het handhavend optreden tegen te onderkennen economische delicten of andere zwaardere strafbare feiten. De verstrekking vindt voorts plaats overeenkomstig het bepaalde in de leden 6 tot en met 8 van artikel 4.13 van de wet.

4. Gevolgen van het besluit (m.u.v. financiële gevolgen)

De gevolgen van dit besluit voor de bescherming van persoonsgegevens zijn inzichtelijk gemaakt in een addendum op de DPIA voor de Wodg (voor deze gevolgen wordt verwezen naar het addendum op de DPIA die bij de internetconsultatie beschikbaar is gesteld). De totstandkoming van dit addendum op de DPIA is een iteratief proces geweest dat parallel liep aan het wetgevingsproces. De inzichten die tijdens het opstellen van dit addendum zijn opgedaan, zijn meegenomen in het ontwerp van dit besluit.

5. Uitvoering

[NB: de gevolgen voor de uitvoering worden gedurende de internetconsultatie nader in kaart gebracht]

---

[17] Artikel 2.10.
[18] Verstrekking in het kader van artikel 6, vierde lid, jo. artikel 23, eerste lid, onder b en d, AVG. Zie ook artikel 8, tweede lid, van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden: het beschermen van de openbare veiligheid en het voorkomen van wanordelijkheden en strafbare feiten.

Met het oog op de invoering van de Wodg en de bijbehorende uitvoeringsregelgeving vindt een uitgebreid implementatie- en communicatietraject plaats binnen Defensie, waarbij allerlei activiteiten worden gepland en uitgevoerd om de organisatie voor te bereiden op de komst van de Wodg.

6. Toezicht en handhaving

Het toezicht op de regels in dit besluit vindt plaats door de Functionaris Gegevensbescherming (hierna: FG) als interne toezichthouder en door de Autoriteit persoonsgegevens (hierna: AP) als externe toezichthouder. In de memorie van toelichting bij het wetsvoorstel is op deze toezichtsystematiek uitgebreid ingegaan.

De bepalingen in hoofdstuk 2 van dit besluit over de gereedstelling beogen – naast de inkadering van de bepalingen uit de wet – de toezichthouders versterkt in staat te stellen om toezicht te houden op de wet en dit besluit. In het bijzonder komt dit tot uitdrukking in twee bepalingen. Het vereiste van machtiging (artikel 2.1, tweede lid) dient ervoor te zorgen dat een beperkte kring van personen voor een bepaald doel toegang heeft tot persoonsgegevens en die ook mag verwerken. Het vereiste van logging (artikel 2.2) zorgt ervoor dat er bij de bevoegdheid van persoonsgerichte kennisvergaring – die een zeer ingrijpende inbreuk maakt op het recht op de persoonlijke levenssfeer – in detail zicht is op de verwerkingen die daarbij plaatsvinden.

De bepalingen in hoofdstuk 3 van dit besluit over de inzet van de krijgsmacht zijn op hoofdlijnen een voortzetting van het bepaalde in de RGMO. De FG en de AP hielden toezicht op die regels, door het op het niveau van algemene maatregel van bestuur tillen van die regels, wordt die toezichtsystematiek niet gewijzigd. Het afwijken van die toezichtsystematiek is op grond van artikel 3, zesde lid, UAVG ook niet mogelijk.

7. Financiële gevolgen

Dit besluit kent op zichzelf geen directe gevolgen voor de rijksbegroting. Dit besluit biedt een nadere uitwerking voor het tijdig gereedstellen van de krijgsmacht. Dit zorgt ervoor dat de gereedstelling niet vertraagd en het mogelijk wordt voor de krijgsmacht om daadwerkelijk afschrikwekkend te zijn en voldoende berekenbaar te zijn bij bondgenootschappelijke ondersteuning.

Het besluit vormt daarom een nadere uitwerking van hoe omgegaan wordt met het wettelijk kader. Zodra dit kader gebruikt wordt zal daarbij een specifieke afweging gemaakt worden waarbij ook aandacht is voor de budgettaire gevolgen. Daarbij geldt dat het ministerie van Defensie als beleidsinitiërend departement en het beleidsverantwoordelijke departement zorg zal dragen voor de benodigde dekking voor de kosten die hieruit voortvloeien, zodat deze kosten worden ingepast in de departementale begrotingen, conform de regels budgetdiscipline.

8. Internetconsultatie

PM: *Onderwerpen die bij de internetconsultatie aan de orde zijn gebracht.*

9. Advies van de Autoriteit persoonsgegevens

PM: *Gedurende internetconsultatie wordt de Autoriteit Persoonsgegevens verzocht om dit concept besluit te toetsen overeenkomstig artikel 36, vierde lid, AVG.*

10. Overgangsrecht en inwerkingtreding

Het besluit voorziet niet in overgangsrecht.

De inwerkingtreding van dit besluit is gelijktijdig met de inwerkingtreding van de wet.

ARTIKELSGEWIJS

Artikel 2.1 (voorwaarden gegevensverwerking)

Eerste lid

Bij de uitvoering van de verschillende taken opgenomen in de wet moet worden voorzien in een functiescheiding tussen deze taken en rollen. Hierbij moet gedacht worden aan een onderscheid tussen de verschillende verwerkingen op grond van de wet. Zo kan de verwerking van persoonsgegevens ten behoeve van het ontwerpen en ontwikkelen van en het experimenteren met materieel, technologieën en technieken niet samengaan met de verwerking ten behoeve van de informatiepositie. De concrete invulling zal plaatsvinden op organisatieniveau en dient nader vastgelegd te worden in werkprocessen, waarbij gedifferentieerd kan worden tussen verschillende type werkzaamheden passend bij de situatie.

Tweede lid

De verwerking van persoonsgegevens op grond van de specifieke taken in de wet dient plaats te vinden door het daartoe gemachtigde defensiepersoneel. Dat betekent dat een machtiging verleend dient te worden voor de verwerking van persoonsgegevens ten behoeve van respectievelijk de informatiepositie, het bewaken en beveiligen van netwerk- en informatiesystemen van defensieonderdelen en het bewaken en beveiligen van militaire objecten en beschermen van het defensiepersoneel. Voor de verwerking van persoonsgegevens op grond van artikel 4.8 van de wet (de gereedstellingsactiviteiten) is een machtiging vereist voor de verwerkingen ten behoeve van het ontwikkelen van opleidings- en trainingsprogramma's en oefenomgevingen (artikel 2.4, tweede lid, van dit besluit) en ten behoeve van het ontwerpen en ontwikkelen van en het experimenteren met materieel, technologieën en technieken (artikel 2.6, eerste en tweede lid, van dit besluit). Voor de overige gereedstellingsactiviteiten is een systeem van machtigingen niet passend en wordt voorzien in andere waarborgen (zie artikel 2.4, vierde lid, van dit besluit).

De machtiging heeft tot doel de kring van personen, die bevoegd zijn om persoonsgegevens te verwerken en toegang verkrijgen tot persoonsgegevens, te beperken tot diegenen voor wie dit, vanwege de taak waarmee zij zijn belast, noodzakelijk is. De machtiging zal gekoppeld worden aan bepaalde functies, waarmee de functionaris gemachtigd zal zijn. Dit zal worden ingericht op '*need to know*' basis. Voor de precieze uitwerking van het systeem van de machtiging wordt aan de organisatie de nodige ruimte gelaten. Dit is van groot belang voor de werkbaarheid van het systeem.

Derde lid

De machtiging bevat een omschrijving van de verwerkingen en bronnen waartoe de functionaris wordt gemachtigd en de onderdelen van de taak ter uitvoering waarvan de verwerkingen worden gedaan.

De machtiging dient een duidelijke omschrijving te bevatten van de verwerkingen waartoe de betreffende functionaris wordt gemachtigd en van de onderdelen van de taak ter uitvoering waarvan de verwerkingen worden verricht. De omschrijving dient er in de eerste plaats toe aan de gemachtigde functionaris helderheid te bieden omtrent zijn bevoegdheden waar het de verwerking van gegevens betreft. In de tweede plaats biedt de machtiging aan de beheerder duidelijkheid omtrent de toegang tot de gegevens die hij voor de betreffende functionaris moet realiseren.

Vierde lid

De functionarissen die tot bepaalde verwerkingen zijn gemachtigd moeten voldoen aan bepaalde deskundigheidseisen. Die eisen worden gesteld voor zover dit voor hun functie relevant is en de inhoudelijke invulling van de eisen kan dan ook per functie verschillen.

In de eerste plaats gaat het hierbij om het informatieproces binnen de defensieonderdelen. Gemachtigde functionarissen dienen bekend te zijn met de verschillende informatieprocessen binnen het respectievelijke defensieonderdeel, ten behoeve waarvan de gemachtigde persoonsgegevens verwerkt, die gevolgd dienen te worden bij die gegevensverwerking. Het gaat dan om processen ten aanzien van de gegevensverwerking die plaatsvindt ten behoeve van het opleiden, trainen en oefenen, het bewaken en beveiligen en de informatiepositie. Voor kennisvergaring ten behoeve van de informatiepositie is het ook van belang op de hoogte te zijn van de processen die van toepassing zijn bij persoonsgerichte kennisvergaring. Ten tweede dienen de gemachtigde functionarissen kennis te hebben van de relevante wet- en regelgeving voor hun functie. Dit heeft in ieder geval betrekking op de Wet op de defensiegereedheid, de Algemene verordening gegevensbescherming, de Uitvoeringswet Algemene verordening gegevensbescherming en dit besluit. Ten derde, moeten de gemachtigde functionarissen bewust zijn van de risico’s die er zijn bij het verwerken van persoonsgegevens. Het gaat daarbij enerzijds om bewustzijn over de inbreuk die kan plaatsvinden voor de persoonlijke levenssfeer van burgers en anderzijds om de risico’s voor Defensie bij de onzorgvuldige omgang met persoonsgegevens.

Artikel 2.2 (logging gegevensverwerking)

Het geautomatiseerd vastleggen van gegevens over de verwerking van persoonsgegevens is een waarborg ter controle van de rechtmatigheid van de gegevensverwerking en ter waarborging van de integriteit en beveiliging van de persoonsgegevens. In dit geval is de loggingplicht opgenomen voor de verwerkingen die plaatsvinden ten behoeve van de persoonsgerichte kennisvergaring. Het gaat hier om een verwerking op basis waarvan een grote inbreuk gemaakt kan worden op het recht op bescherming van de persoonlijke levenssfeer. Bij het verzamelen, wijzigen, raadplegen, verstrekken of verwijderden van deze persoonsgegevens dient geregistreerd te worden wie heeft verwerkt en op welk moment (datum en tijdstip) die verwerking plaatsvond.

De vastgelegde gegevens kunnen uitsluitend worden gebruikt voor controledoeleinden. Deze controles kunnen intern of extern van aard zijn, maar hebben als doel om de naleving van de bij

of krachtens de wet gestelde normeringen te controleren en mogen dus niet voor andere doeleinden worden ingezet.

Artikel 2.3 (verlenging bewaartermijn)

Eerste lid

Met deze bepaling wordt de procedure voor het verlengen van de bewaartermijn geregeld. Een verzoek om de bewaartermijn te verlengen wordt ingediend bij de verwerkingsverantwoordelijke – de Minister van Defensie. Dit verzoek wordt ingediend door de Commandant der Strijdkrachten (CDS), die de militaire verantwoordelijkheid draagt voor de gereedstelling en de inzet van de krijgsmacht. In de praktijk kan de CDS de uitvoering hiervan mandateren.

Na afloop van de verlengde bewaartermijn kan op grond van artikel 4.7, tweede lid, van de wet, nog eenmaal een nieuw verzoek om verlenging van de bewaartermijn worden ingediend, met dien verstande dat deze termijn eveneens met ten hoogste twee jaar verlengd kan worden.

Tweede lid

De commandant dient bij het verzoek om verlenging een aantal gegevens aan te leveren. Deze gegevens zijn relevant voor de beoordeling van de noodzaak van verlenging en verplichten tot evaluatie van de bewaarde persoonsgegevens.

Het eerste onderdeel (onderdeel a) is een beschrijving van de gegevensverzameling waarin de persoonsgegevens zich bevinden waarvoor om een verlenging van de bewaartermijn wordt verzocht. De aanduiding is relevant omdat in veel gevallen persoonsgegevens niet geïsoleerd bewaard worden, maar onderdeel zijn van een gegevensverzameling. De gegevensverzameling kan worden aangevuld en gewijzigd met persoonsgegevens. Voor de bewaartermijn is dan de oudste eerste verwerking van persoonsgegevens bepalend. Bij de beoordeling van de verlenging van de bewaartermijn gaat het uitsluitend om de persoonsgegevens in die gegevensverzameling, maar indien geoordeeld wordt dat de bewaartermijn niet verlengd wordt kan dit wel gevolgen hebben voor de waarde van de gegevensverzameling.

Daarnaast dient in het verzoek te worden aangegeven of het om bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard gaat bij de persoonsgegevens waarvoor om verlenging wordt verzocht (onderdeel b). Daarbij dient ook te worden aangegeven of die gegevens incidenteel voorkomen of dat veel van deze categorieën van persoonsgegevens zich in de gegevensverzameling bevinden. Aan bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard wordt een hoger niveau van bescherming toegekend in de Wet op de defensiegereedheid dan ‘gewone’ persoonsgegevens.

Het verzoek dient ook een beschrijving te bevatten van het doel waarvoor de persoonsgegevens zijn verwerkt (onderdeel c). Het gaat daarbij om een van de volgende doelen: gereedstellingsactiviteit, informatiepositie en bewaken en beveiligen. Binnen die activiteiten dient ook aangegeven te worden welke specifieke subactiviteit het betreft, bijvoorbeeld het beveiligen van netwerk- en informatiesystemen van defensieonderdelen.

Voorts wordt in het verzoek aangegeven gedurende welke periode de persoonsgegevens sinds de eerste verwerking reeds zijn bewaard (onderdeel d).

De noodzaak, proportionaliteit en subsidiariteit van het verlengen van de bewaartermijn dient onderbouwd te worden (onderdeel e). Het gaat daarbij om de vraag hoe en waarom deze

persoonsgegevens nog steeds bijdragen aan het doel waarvoor deze zijn verwerkt. De onderbouwing hiervan zal per doel verschillen, echter kan met betrekking tot persoonsgerichte kennisvergaring worden aangesloten bij de factoren uit het vierde lid. In het verzoek dient tevens te worden onderbouwd dat het verzoek om verlenging vanuit de daarmee gepaard gaande beperking van het recht op bescherming van de persoonlijke levenssfeer van de personen wier gegevens het betreft proportioneel en subsidiair is. Bij de proportionaliteitsafweging wordt het belang van de gereedheid van het militair vermogen van de krijgsmacht om persoonsgegevens langer te kunnen gebruiken afgewogen tegen de inbreuk op de persoonlijke levenssfeer die daarmee gepaard gaat, ook hier wordt dit in het licht van de factoren uit het derde lid bezien. Bij de subsidiariteitsafweging moet worden onderbouwd dat het verlengen van de bewaartermijn het minst ingrijpende middel is om het doel — het kunnen blijven gebruiken van de gegevens voor de oorspronkelijke activiteit — te bereiken, en dat dit minder inbreuk maakt dan het alternatief van het opnieuw verzamelen van persoonsgegevens.

Ook wordt een aanduiding gegeven van het gebruik van de persoonsgegevens in de afgelopen periode (onderdeel f).

Derde lid

De aangeleverde gegevens bij het verzoek om verlenging zijn leidend bij het beoordelen van dit verzoek door de Minister van Defensie. Bij die beoordeling dient het belang van het langer bewaren ten behoeve van de gereedheid afgewogen te worden tegen het belang van de persoonlijke levenssfeer van betrokkene. Bij die afweging is relevant welke gevolgen de verlenging heeft voor de bescherming van de persoonlijke levenssfeer van betrokkene. Daartegenover staat het belang van de krijgsmacht en in het concrete geval het specifieke doel waarvoor de gegevens zijn verwerkt. De noodzaak van dat doel moet nog steeds bestaan.

Bij de vraag inzake de noodzakelijkheid kan bij gereedstellingsactiviteiten bijvoorbeeld gedacht worden aan in hoeverre de persoonsgegevens nog actuele toegevoegde waarde hebben voor het specifieke doel en, in het bijzonder bij het bewaken en beveiligen, of de persoonsgegevens betrekking hebben op bestaande dreigingen voor de veiligheid en gereedheid van de defensieonderdelen.

Bij de afweging dient aan het belang van betrokkene zwaarder gewicht toegekend te worden als het bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard betreft. Deze persoonsgegevens hebben op basis van artikel 4.5 Wodg meer bescherming en daar moet dientengevolge ook rekening mee gehouden worden bij de verlenging van de bewaartermijn. In het verlengde daarvan kan het treffen van bepaalde maatregelen zoals dataminimalisatie en pseudonimiseren, waar dit verenigbaar is met het doel van de verwerking, bijdragen aan de proportionaliteit van het langer bewaren van bepaalde persoonsgegevens.

Vierde lid

Voor de beoordeling van het verlengen van de bewaartermijn van persoonsgegevens die verwerkt zijn voor het doel van de persoonsgerichte kennisvergaring gelden specifieke factoren waar bij die beoordeling rekening mee gehouden moet worden. Deze factoren vormen een onderdeel van de beoordeling van de noodzaak van de verlenging zoals opgenomen in het derde lid. Met deze specifieke factoren wordt de beoordeling ingekaderd voor de grotere inbreuk op het recht van bescherming van de persoonlijke levenssfeer die door de persoonsgerichte kennisvergaring gemaakt wordt.

Bij de onderdelen a tot en met e gaat het om factoren die bijdragen aan het vormen van een beeld over of er nog steeds een noodzaak bestaat de specifieke persoonsgegevens te bewaren. Het gaat er dan om of het nog waarschijnlijk is dat de krijgsmacht in de relevante operationele omgeving zal optreden, welke dreiging vanuit de personen gaat (voor zover het om personen, bedoeld in artikel 4.9, vierde lid, onderdeel a, Wodg, gaat), of de personen nog relevant zijn (bijvoorbeeld persoon x is niet langer burgemeester in plaats y).

De laatste factor is hoe waarschijnlijk het is dat de persoonsgegevens opnieuw verzameld zouden worden voor dat doel. Indien op grond van de onderdelen a tot en met e een beeld ontstaat dat de persoonsgegevens noodzakelijk zijn voor het doel van de persoonsgerichte kennisvergaring dan speelt deze factor een rol. Een positief antwoord op deze vraag geeft een indicatie van de noodzaak, waarbij het onwenselijk is dat de gegevens opnieuw voor hetzelfde doel verzameld worden. Overigens is het opnieuw verzamelen van dezelfde persoonsgegevens niet noodzakelijk (in de zin van de Wet op defensiegereedheid) als de persoonsgegevens reeds verzameld zijn en de bewaartermijn op grond van deze bepaling verlengd had kunnen worden. Ook het feit dat bepaalde persoonsgegevens niet opnieuw kunnen worden verzameld omdat ze niet langer bestaan kunnen een factor zijn om die gegevens langer te bewaren.

Artikel 2.4 (opleiden, trainen en oefenen)

Eerste lid

De activiteiten die de defensieonderdelen verrichten zijn op grond van de Wet op de defensiegereedheid steeds gericht op het verzekeren van de gereedheid van het militair vermogen van de krijgsmacht. Om dit te bereiken wordt, onder meer, defensiepersoneel opgeleid en getraind en dient de geoefendheid onderhouden te worden. In dat kader is het relevant dat het militair vermogen ook geloofwaardig en doeltreffend ingezet moet kunnen worden. Dat vereist in bepaalde gevallen dat in de publieke ruimte wordt geoefend om een afschrikkende werking te hebben (waarmee wordt beoogd daadwerkelijke inzet te voorkomen).

Het opleiden, trainen en oefenen vindt plaats binnen de gereedstellingssystematiek.[19] De gereedstellingssystematiek geeft in beginsel invulling aan de proportionaliteit van de verwerking van persoonsgegevens bij deze activiteiten. Op grond daarvan wordt pas op het vierde niveau en tijdens de certificeringsoefening in de openbare ruimte getraind. Daarmee wordt beoogd dat het defensiepersoneel pas op het moment dat zij voldoende kennis hebben en daarmee ook verantwoord met persoonsgegevens kunnen omgaan daarmee in aanraking komen.

Om binnen de gereedstellingssystematiek het doel van het verzekeren van de gereedheid van het militair vermogen van de krijgsmacht te bereiken is het noodzakelijk dat het defensiepersoneel in de operationele oefenomgeving zo realistisch en goed mogelijk kan trainen en oefenen. Met het oog daarop dienen opleidings- en trainingsprogramma's en oefenomgevingen te worden ontwikkeld die dit doel kunnen bereiken. Hiermee wordt bewerkstelligd dat alleen in specifieke situaties gedurende opleiding, training en oefening persoonsgegevens (in voorkomend geval als bijvangst) worden verwerkt.

---

[19] Zie uitgebreid hoofdstuk 2 van de memorie van toelichting op de Wet op de defensiegereedheid (PM kamerstuk nummer).

Tweede lid

Voor het ontwikkelen van opleidings- en trainingsprogramma's en oefenomgevingen zijn gegevens noodzakelijk om deze zo realistisch mogelijk te maken. Daar kunnen gegevensverzamelingen voor gebruikt worden. Die gegevensverzamelingen kunnen persoonsgegevens bevatten, echter zijn die gegevens over specifieke personen niet relevant voor dit doel. Desalniettemin dragen persoonsgegevens als input bij aan het ontwikkelen van deze opleidings- en trainingsprogramma's en oefenomgevingen omdat daarmee de realiteit beter benaderd kan worden.

Het verwerken van persoonsgegevens ten behoeve van het ontwikkelen van een opleidings- en trainingsprogramma of oefenomgeving vindt uitsluitend plaats voor zover dat noodzakelijk is voor dit doel en door de functionarissen die daartoe zijn gemachtigd. Zie verder de toelichting bij artikel 2.1, tweede lid.

Derde lid

Voor de ingebruikname van het opleidings- of trainingsprogramma of de oefenomgeving dienen redelijke maatregelen getroffen worden zodat deze persoonsgegevens zijn verwijderd, geanonimiseerd of gepseudonimiseerd. Bij redelijke maatregelen dient meegenomen te worden wat de stand van de techniek toelaat en de uitvoeringskosten[20] die met de handeling gepaard gaan. Ten aanzien van het pseudonimiseren zij vermeld dat de gebruikers van het programma of de omgeving – niet zijnde de ontwikkelaars – geen toegang mogen hebben tot de aanvullende gegevens waarmee de persoonsgegevens alsnog aan een betrokkene gekoppeld kunnen worden.

Vierde lid

Binnen de gereedstellingssystematiek wordt in beginsel tot en met het derde niveau gewerkt met opleidings- en trainingsprogramma's en oefenomgevingen. Op het moment dat buiten die gecreëerde omgeving wordt opgeleid of getraind, worden aanvullende voorwaarden gesteld voor de activiteiten waar het verwerken van persoonsgegevens een belangrijk onderdeel van vormt. Het gaat hierbij om het opleiden en trainen voor activiteiten waar het verwerken van persoonsgegevens een essentieel onderdeel van is. Om die reden is deze bepaling niet van toepassing op de activiteiten genoemd in artikel 4.8, eerste lid, onderdeel a, Wodg. Daarvoor gelden de specifieke voorwaarden uit artikel 2.5 van dit besluit. Voor het verrichten van deze activiteiten is vereist dat de personen die de opleiding of training volgt theoretische kennis heeft over hoe op een correcte en verantwoorde wijze persoonsgegevens worden verwerkt. Daarnaast dient deze activiteit onder toezicht plaats te vinden van een persoon met kennis en ervaring in het verwerken van persoonsgegevens.

Artikel 2.5 (gebruik van materieel en technische hulpmiddelen)

Eerste lid

[20] Het ontbreken van of een beperkt budget zijn geen gegronde reden om hier geen uitvoering aan te geven. Het gaat erom dat de kosten in redelijke verhouding moeten staan tot de inspanning.

Voor een doeltreffend optreden in de operationele omgeving is in de hedendaagse oorlogsvoering vereist dat het nieuwste defensiematerieel, waaronder de modernste technologieën, gebruikt kan worden. Hierbij valt te denken aan allerlei bemande en onbemande voertuigen, vaartuigen en luchtvaartuigen die gebruik maken van allerlei sensoren om operationeel te zijn. Zonder die sensoren of waarneming via camera's is het gebruik niet mogelijk. Het gaat hier daarom primair om het daadwerkelijk kunnen rijden, varen en vliegen met het materieel. Bij het gebruik verwerken die sensoren in bepaalde gevallen ook persoonsgegevens die geen doel hebben voor het gebruik van het materieel zelf (bijvangst).

Voor de gereedheid van het militair vermogen van de krijgsmacht is het noodzakelijk dat het defensiepersoneel gereedstellingsactiviteiten kan verrichten met defensiematerieel. Voor het gebruik van dit materieel mogen persoonsgegevens verwerkt worden. Die persoonsgegevens mogen niet meer verwerkt worden na het gebruik van het materieel. Een andere verwerking mag alleen plaatsvinden indien de persoonsgegevens op zijn minst geanonimiseerd zijn.

Tweede lid

Onderdeel van het opleiden, trainen en oefenen is ook het gebruik van allerlei technische hulpmiddelen om de omgeving waar te nemen en om gebruik te maken van het elektromagnetisch spectrum. Deze technische hulpmiddelen, veelal sensoren, kunnen zich op bemande en onbemande voertuigen, vaartuigen en luchtvaartuigen bevinden en gebruikt worden. Maar technische hulpmiddelen kunnen ook los daarvan gebruikt worden, hierbij valt ook te denken aan het gebruik binnen het elektromagnetisch spectrum. Het ongereguleerd gebruik kan een aanzienlijke inbreuk op de persoonlijke levenssfeer meebrengen, om die reden worden daaraan bijzondere regels gesteld. Het gaat hierbij om een specifieke bepaling voor het materieel dat gebruikt wordt met het oogmerk van het waarnemen van de omgeving of het gebruik van het elektromagnetisch spectrum. Het gebruik van materieel om te kunnen rijden, varen en vliegen valt onder het eerste lid, waarbij geen voorwaarden worden verbonden aan de fysieke locatie. Dat is ook niet passend bij bijvoorbeeld vliegtuigen.

Op grond van deze bepaling wordt het gebruik van technische hulpmiddelen om de omgeving waar te nemen en om gebruik te maken van het elektromagnetisch spectrum in beginsel beperkt tot op of boven militaire objecten. Het uitgangspunt dat deze activiteit plaatsvindt op een afgesloten plek komt voort uit de gereedstellingssystematiek, waarbij alleen waar het echt noodzakelijk is buiten de terreinen wordt opgeleid, getraind en geoefend. Dit hangt samen met de vereisten van proportionaliteit en subsidiariteit waaraan dient te worden voldaan. Het gebruik van technische hulpmiddelen op of boven deze plaatsen maakt niet dat de effecten van het gebruik zich altijd zullen beperken tot de geografische grens daarvan, dit is praktisch niet haalbaar. De gedachte is dat het gebruik van deze technische hulpmiddelen zich uitsluitend richt op de personen die zich op of boven het militaire object bevinden.

Derde lid

Gereedstellingsactiviteiten vinden vanuit de gereedstellingssystematiek pas buiten de militaire oefenterreinen plaats wanneer de betrokken personen over voldoende kennis en vaardigheden beschikken om in 'de echte wereld' te trainen. Het buiten militaire terreinen opleiden, trainen en oefenen is noodzakelijk voor het zo realistisch mogelijk uitvoeren van die activiteiten en te zorgen dat de militair daadwerkelijk gereed is. Om te zorgen dat ook de verwerking van persoonsgegevens bij deze activiteiten beperkt blijft tot het strikt noodzakelijke worden daarvoor regels gesteld.

Voor zover een opleiding, training of opleiding buiten een militair terrein plaatsvindt dan mogen deze technische hulpmiddelen alleen ingezet worden als dit gericht is op de personen die onderdeel uitmaken van de opleiding, training of oefening. Het gaat daarbij in voorkomend geval om de militair ambtenaar, maar kan ook betrekking hebben op ingehuurde derden, zoals instructeurs of rollenspelers.

Persoonsgegevens van andere personen dan de deelnemers aan de specifieke activiteit van de opleiding, training of oefening (gewone burgers) dienen niet verzameld te worden, maar kunnen met sensoren als bijvangst toch verwerkt worden. Daarbij wordt waar mogelijk ook ingezet op het gebruik van *privacy-enhancing technologies*, maar is het verwerken van persoonsgegevens niet uitgesloten. Voor de gevallen waar duidelijk is dat het verwerken van persoonsgegevens een aanzienlijke inbreuk oplevert dan dienen die persoonsgegevens direct verwijderd en vernietigd te worden. Het criterium is daarbij of die persoonsgegevens redelijkerwijs voorzienbaar een min of meer volledig beeld van bepaalde aspecten van iemands privéleven geven. Met dit criterium wordt aangesloten bij hetgeen hierover is bepaald in de toelichting op artikel 4.2, derde lid, Wodg.

Indien op voorhand duidelijk is dat een handeling ten tijde van een specifieke activiteit van de opleiding, training of oefening meebrengt dat daarmee ook persoonsgegevens verzameld worden die een min of meer volledig beeld van bepaalde aspecten van iemands privéleven geven dan dient die handeling niet plaats te vinden, tenzij dit onvermijdelijk is voor de goede uitvoering van die activiteit. Indien gedurende de handeling of daarna duidelijk is dat persoonsgegevens zijn verzameld die een aanzienlijke inbreuk maken op de persoonlijke levenssfeer dan mogen deze niet verder gebruikt worden als onderdeel van die activiteit (of andere doeleinden) en dienen deze onverwijld verwijderd te worden. De beoordeling of sprake is van een aanzienlijke inbreuk dient uiterlijk plaats te vinden voor de eerstvolgende verwerking met betrekking tot de persoonsgegevens nadat deze zijn verzameld.

De persoonsgegevens die niet aan dat criterium voldoen mogen verwerkt worden conform de bepalingen uit de Wet op de defensiegereedheid. Uiteindelijk dienen ook die persoonsgegevens verwijderd te worden, maar kunnen nog onderdeel zijn van de specifieke activiteit en bijvoorbeeld meegenomen worden bij de geïntegreerde commandovoering of de evaluatie van de activiteit. Dit betekent dat het realistisch oefenen tijdelijk ten koste kan gaan van de bescherming van de persoonlijke levenssfeer van niet deelnemers aan een specifieke activiteit van een opleiding, training of oefening.

Het gebruik van bemande en onbemande voertuigen, vaartuigen en luchtvaartuigen moet op basis van beleid van het Ministerie van Defensie plaatsvinden. Dit beleid moet ertoe dienen dat er richtlijnen worden opgesteld over de wijze waarop bijvoorbeeld drones worden gebruikt in de publieke ruimte alsmede hoe omgegaan wordt met de gegevens (in aanvulling op de Wet op de defensiegereedheid en dit besluit). Bij de richtlijnen kan betreffende drones bijvoorbeeld aangesloten worden bij de gedragscode van het Europees Agentschap voor de veiligheid van de

luchtvaart (EASA) over privacy bij het gebruik van drones.[21] In lijn daarmee kan het beleid onderscheid maken tussen de openbare publieke ruimte, privé (zoals boven woonwijken) en andere plekken, zodat hier rekening mee kan worden gehouden bij de routes ten tijde van de opleiding, training of oefening. Daarnaast zouden de aandachtspunten van de Artikel 29-werkgroep (opgevolgd door het Europees Comité voor gegevensbescherming) uitgewerkt kunnen worden.[22] Tenslotte dient het gebruik van *privacy-enhancing* technologie waar verenigbaar met het doel van de opleiding, training of oefening te worden bevorderd.

Artikel 2.6 (ontwerpen, ontwikkelen en experimenteren)

Eerste lid

Het ontwerpen en ontwikkelen van en het experimenteren met materieel, technologieën en technieken kan betrekking hebben op tastbare voorwerpen, zoals een vuurwapen of een tank. Het ontwerpen en ontwikkelen hiervan en het experimenteren hiermee kan veelal in een geïsoleerde omgeving plaatsvinden, waarbij geen persoonsgegevens verwerkt zullen worden. De moderne oorlogsvoering kan echter niet los gezien worden van allerlei digitale ontwikkelingen met software (inclusief firmware). Bij het ontwerpen en ontwikkelen hiervan en het experimenteren hiermee zijn gegevens randvoorwaardelijk om te zorgen dat bij de daadwerkelijke inzet daarvan veilig en doeltreffend gehandeld kan worden. Dat wil zeggen dat het veilig is voor het personeel van de krijgsmacht zelf en dat burgerslachtoffers worden voorkomen. Daarbij wordt waar mogelijk gekozen voor de methoden en middelen die de geringste inbreuk maken op de persoonlijke levenssfeer en geschikt zijn om de doelen te bereiken, bijvoorbeeld door gebruik te maken van synthetische gegevens.

Ten behoeve van het ontwerpen en ontwikkelen van en het experimenteren met materieel, technologieën en technieken mogen persoonsgegevens slechts verwerkt worden voor zover technische maatregelen getroffen worden om de gegevens te verwijderen, anonimiseren of pseudonimiseren. Naar gelang het specifieke doel van het ontwerpen, ontwikkelen of experimenteren wordt daarin een keuze gemaakt die recht doet aan het doel en de bescherming van de persoonlijke levenssfeer van betrokkene. Het gaat daarbij om alle redelijke maatregelen, dat wil zeggen dat het pseudonimiseren van persoonsgegevens en de tijd en kosten die daarmee gepaard gaan in redelijke verhouding moeten staan tot het beschermen van de persoonsgegevens van betrokkenen, daarbij rekening houdend dat aan bijzondere categorieën van persoonsgegevens meer bescherming toekomt.

Tweede lid

Voor het ontwikkelen van artificiële intelligentie-systemen (hierna: AI-systemen) die gebruikt kunnen worden in de militaire context is des temeer vereist dat die systemen betrouwbaar en veilig gebruikt kunnen worden. AI-systemen kunnen de commandant, onder andere, ondersteunen in het maken van snelle beslissingen. Hoewel deze op basis van de output van het

---

[21] European Union Aviation Safety Agency, 'Code of Conduct', easa.europa.eu, https://www.easa.europa.eu/en/domains/civil-drones/privacy/code-of-conduct.
[22] Groep voor de bescherming van personen in verband met de verwerking van persoonsgegevens, *Advies 1/2015 over vraagstukken betreffende privacy en gegevensbescherming in verband met het gebruik van drones*, juni 2015, paragraaf 3.6.

AI-systeem zelf een verantwoorde keuze dient te maken, zal die keuze (deels) gebaseerd zijn op de geleverde output. Het is daarom uitermate belangrijk dat de AI-systemen ontwikkeld worden op basis van kwalitatief hoogwaardige data. Hierbij wordt waar mogelijk ook gebruik gemaakt van synthetische of geanonimiseerde data, maar is niet uitgesloten dat ook (niet gepseudonimiseerde) persoonsgegevens onderdeel vormen van die kwalitatief hoogwaardige data.

Deze bepaling beoogt een balans te vinden tussen het belang wat gediend wordt met het ontwikkelen van een AI-systeem en de bescherming van de persoonlijke levenssfeer. Dit betekent dat het enerzijds mogelijk is persoonsgegevens te gebruiken voor dat doel, maar anderzijds dat vereisten worden gesteld aan het gebruik daarvan. Die persoonsgegevens moeten namelijk zorgen dat een gegevensverzameling (dataset) relevant, voldoende representatief voor het beoogde doel van het AI-systeem en zoveel mogelijk foutenvrij is. Daarnaast is die gegevensverzameling gericht op het veilig en beoogd gebruik van het AI-systeem. Met het oog op het gebruik van een AI-systeem dienen de persoonsgegevens die verwerkt zijn voor het trainen, testen of valideren van het AI-systeem niet langer herleidbaar te zijn tot een persoon voorafgaand aan ingebruikname. Daartoe dienen technische maatregelen getroffen te worden om de gegevens te verwijderen of anonimiseren. Zie nader de toelichting op het eerste lid.

Bij het begrip artificiële intelligentie-systeem wordt aangesloten bij de begripsbepaling zoals dat ook is opgenomen in artikel 3, onderdeel 1, van de Verordening artificiële intelligentie.[23] Die verordening is niet van toepassing op AI-systemen die uitsluitend verhandeld of gebruikt worden voor militaire, defensie- of nationale veiligheidsdoeleinden.[24] De daarin opgenomen begripsbepaling is neutraal en toekomstbestendig geformuleerd en daardoor ook toepasbaar in de militaire context.

Derde lid

Het ontwikkelen en gebruik van AI-systemen dient plaats te vinden met inachtneming van de beginselen voor verantwoord gebruik van artificiële intelligentie. Als uitgangspunt worden hiervoor gehanteerd de beginselen inzake verantwoord gebruik van artificiële intelligentie voor defensiedoeleinden van de Noord-Atlantische Verdragsorganisatie.[25] De NAVO-beginselen komen voort uit de ethische, juridische en beleidskaders van de NAVO-verdragsstaten. Deze beginselen worden ook breder op vergelijkbare wijze onderschreven door, onder andere, de

---

[23] Verordening (EU) 2024/1689 van het Europees Parlement en de Raad van 13 juni 2024 tot vaststelling van geharmoniseerde regels betreffende artificiële intelligentie en tot wijziging van de Verordeningen (EG) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 en (EU) 2019/2144, en de Richtlijnen 2014/90/EU, (EU) 2016/797 en (EU) 2020/1828 (PbEU 2024, L). Vergelijkbaar met de begripsbepaling van de Organisatie voor Economische Samenwerking en Ontwikkeling in *Recommendation of the Council on Artificial Intelligence*, 2024.
[24] Artikel 2, derde lid, van de Verordening artificiële intelligentie.
[25] NATO, *Summary of the NATO Artificial Intelligence Strategy*, 2021.

deskundigengroep op hoog niveau inzake kunstmatige intelligentie,[26] de Organisatie voor Economische Samenwerking en Ontwikkeling[27] en de Global Commission on Responsible AI in the Military Domain.[28] Daarnaast zijn het ook de hoofdelementen die in het witboek van het Europees Defensieagentschap over betrouwbare AI voor defensiedoeleinden naar voren komen.[29] Deze beginselen sluiten ook aan bij de Defensie Strategie Data Science en AI.[30]

De beginselen zijn breed geformuleerd en zijn daarom een geschikt kader voor een technologie die sterk in ontwikkeling is. Het ontwikkelen en gebruik van AI-systemen dient op een *rechtmatige wijze* te gebeuren, dit betekent dat gehandeld wordt binnen de bestaande juridische kaders. *Zorgvuldig* ziet op de gepaste zorgvuldigheid en de daarbij behorende oordeelsvorming, waarbij de gebruiker de verantwoording draagt voor de uitkomsten (de eindverantwoordelijke). De ontwikkeling en het gebruik van een AI-systeem moet ook *begrijpelijk* en *transparant* zijn. Het gaat hier om het kunnen verklaren van de technische processen en de daaraan gerelateerde menselijke beslissingen alsmede het kunnen herleiden van de gebruikte gegevenssets en processen waarop een uitkomst is gebaseerd. Het gebruik van een AI-systeem dient beperkt te zijn tot duidelijk omschreven *doeleinden* en moet op een *betrouwbare* wijze plaats kunnen vinden. De betrouwbaarheid veronderstelt dat het gebruik te allen tijde veilig, beveiligd en robuust is. Het gebruik van een AI-systeem dient *controleerbaar* te zijn en menselijk ingrijpen moet mogelijk zijn (*beheersbaar*). Het gaat hier om de menselijke controle waarmee de gebruiker zijn verantwoordelijkheid kan bewerkstelligen. Ten slotte moet (onbedoelde) *vooringenomenheid* zoveel mogelijk voorkomen worden, waarvoor proactief maatregelen getroffen dienen te worden om dit tot een minimum te beperken.

Artikel 2.7 (persoonsgerichte kennisvergaring op aanwijzing)

Eerste lid

Een aanwijzing voor de persoonsgerichte kennisvergaring wordt door de Minister van Defensie gegeven. In de praktijk zal deze hiertoe verzocht kunnen worden door de Commandant der Strijdkrachten (CDS). De CDS stuurt de krijgsmacht aan. Vanuit zijn functie draagt de CDS de militaire verantwoordelijkheid voor de gereedstelling en de inzet van de krijgsmacht.

Tweede lid

De aanwijzing van de Minister van Defensie dient een aantal onderdelen te beschrijven met het oog op de afbakening. Die onderdelen hebben betrekking op de noodzaak, proportionaliteit en subsidiariteit van de aanwijzing.

---

[26] Deskundigengroep op hoog niveau inzake kunstmatige intelligentie, *Ethische richtsnoeren voor betrouwbare KI*, 2019
[27] Organisation for Economic Co-operation and Development, *Recommendation of the Council on Artificial Intelligenc*e, 2024.
[28] The Global Commission on Responsible Artificial Intelligence in the Military Domain, *Responsible by Design: Strategic Guidance Report on the Risks, Opportunities, and Governance of Artificial Intelligence in the Military Domain*, The Hague, 2025, p. 40-41.
[29] European Defence Agency, *White Paper Trustworthiness For AI in Defence: Developing Responsible, Ethical, and Trustworthy AI Systems for European Defence*, 2025.
[30] Ministerie van Defensie, *Defensie Strategie Data Science en AI 2023-2027*, 2023.

Het eerste onderdeel (onderdeel a) vereist dat de achtergrond voor de aanwijzing wordt beschreven. Welke feiten brengen mee dat er in een bepaald geval kennis vergaard dient worden; hoe verhoudt de persoonsgerichte kennisvergaring zich tot het veilig en doeltreffend optreden van de eenheid of het onderdeel van de krijgsmacht in de relevante operationele omgeving. Het gaat dan om de dreigingen die er voor het Koninkrijk of een bondgenoot zijn. Dit kan ondersteund worden met een dreigingsappreciatie van de MIVD. Daarnaast dient te worden beschreven in welk kader de krijgsmacht naar verwachting mogelijk zal optreden waarvoor persoonsgerichte informatie dient te worden verzameld. Hier valt te denken aan een specifieke operatie in NAVO verband, een evacuatie van burgers (*Non-combatant Evacuation Operation*) of de algemene voorbereiding in het kader van hoofdtaak 1.

Met het tweede onderdeel (onderdeel b) dient afgebakend te worden in welk gebied de kennisvergaring omtrent personen mag plaatsvinden. Het kan hier gaan om een geografische of een digitale afbakening. Het focusgebied wordt waar mogelijk zo concreet mogelijk beschreven. Bij de geografische afbakening is dit ten minste op het niveau van een bestuurlijke regio (een provincie of een daarmee vergelijkbare bestuurlijke regio).

Het derde onderdeel (onderdeel c) ziet op het oogmerk waarom persoonsgericht gegevens worden vergaard. Dit ligt in het verlengde van onderdeel a en bevat een noodzakelijkheidstoets van het persoonsgericht vergaren van kennis in verhouding tot het doel daarvan.

De aanwijzing dient te verduidelijken op welke categorie(ën) van personen de kennisvergaring is gericht (onderdeel d). Dat wil zeggen: a. personen die vermoedelijk een gevaar vormen voor de veiligheid van de krijgsmacht of de militaire taakuitoefening van de betrokken eenheden; b. personen in de operationele omgeving die de krijgsmacht mogelijk kunnen ondersteunen; of c. personen die in de operationele omgeving beschermd moeten worden. Deze duiding is relevant omdat op basis van de noodzakelijkheidstoets een aanwijzing voor het vergaren van kennis over de derde categorie van personen doorgaans voor een kortere duur verleend dient te worden dan voor de personen uit de eerste categorie.

Alleen specifieke eenheden mogen persoonsgericht kennis vergaren (onderdeel e). Het aantal personen dat hieraan uitvoering mag geven dient beperkt te zijn gezien de ingrijpendheid van de bevoegdheid. Daaraan draagt ook de functiescheiding uit artikel 2.1, eerste lid, bij.

Derde lid

De Minister van Defensie geeft een aanwijzing indien deze van oordeel is dat de persoonsgerichte kennisvergaring in het desbetreffende geval noodzakelijk is voor een veilig en doeltreffend optreden van eenheden of onderdelen van de krijgsmacht in de relevante operationele omgeving.

Vierde lid

Die aanwijzing kan voor maximaal een jaar worden gegeven. Bij de duur van de aanwijzing betrekt de Minister de proportionaliteit van die aanwijzing, in ieder geval rekening houdend met de categorieën van personen die het betreft. De aanwijzing kan steeds verlengd worden voor ten hoogste een jaar.

Vijfde lid

De verlenging van de aanwijzing dient een aantal elementen te bevatten aanvullend op de initiële aanwijzing. Het gaat daarbij om de noodzaak van de verlenging en de afstemming die

plaatsvindt met de MIVD. De afstemming is noodzakelijk omdat hoe langer kennis over specifieke personen vergaard wordt hoe aannemelijker het is dat deze persoon in het onderzoeksgebied van de dienst valt. Ten slotte kan bij de verlenging ook de bevoegdheid voor de persoonsgerichte kennisvergaring worden overgedragen aan een andere militaire eenheid indien daartoe aanleiding bestaat.

Artikel 2.8 (persoonsgerichte kennisvergaring door de commandant)

Eerste lid

De bevoegdheid van de commandant om op eigen initiatief kennis te vergaren over specifieke personen komt voort uit het grondbeginsel 'freedom of effort' en is een essentieel onderdeel van de opdrachtgerichte commandovoering. Om de aan de commandant opgedragen doelstellingen te realiseren is een bepaalde mate van vrijheid van handelen vereist, om te kunnen anticiperen op onvoorziene situaties of op nieuwe kansen.[31]

De vrijheid van handelen bestaat in de context van het persoonsgericht kennis vergaren uitsluitend in de situaties waarbij een aanwijzing van de Minister van Defensie niet afgewacht kan worden. Het moet in dat verband gaan om spoedeisende en gewichtige redenen die gebruik van de bevoegdheid rechtvaardigen. Hiervan kan sprake zijn in de gevallen waarbij op basis van bepaalde ontwikkelingen met spoed een omgevingsbeeld gevormd moet worden. In het bijzonder gaat het daarbij om onvoorzienbare speciale operaties en evacuaties (*Non-Combatant Evacuation Operation*), maar ook tijdens de uitvoering van een reguliere oefening kan het initiatief van de commandant noodzakelijk zijn. Hierbij valt te denken aan situaties waar gedurende een oefening onbekende of verdachte schepen op zee op de radar in beeld komen of dat onbemande luchtvaartuigen zoals drones waargenomen worden. Een commandant moet in deze gevallen direct een inschatting kunnen maken of er sprake is van een dreiging en zo ja hoe acuut die dreiging is en of daarop handelen noodzakelijk is.

Het initiatief is beperkt tot commandanten die het bevel voeren over een militaire eenheid. In de praktijk kan dit bij speciale eenheden om een commandant gaan die het bevel voert over een groep of ploeg. Bij andere dan speciale eenheden gaat het om de commandant die het bevel voert over ten minste een bataljon of afdeling.

Tweede lid

Direct nadat de commandant gebruik heeft gemaakt van het initiatief om kennis te vergaren over specifieke personen wordt de Minister van Defensie onverwijld om goedkeuring verzocht. Uit artikel 4.9, vijfde lid, Wodg volgt dat de goedkeuring binnen zeven dagen na het gebruik moet zijn gegeven, anders is de goedkeuring onthouden.

Het verzoek om goedkeuring is vergelijkbaar met de aanwijzing, met dien verstande dat in het bijzonder gemotiveerd moet worden waarin de urgentie van het initiatief is gelegen en welke omstandigheden het gebruik daarvan rechtvaardigen met het oog op het veilig en doeltreffend optreden van de eenheid of het onderdeel in de relevante operationele omgeving.

---

[31] Ministerie van Defensie, *Joint Doctrine Publicatie 5 – Commandovoering*, 2012, p. 33.

Derde lid

De Minister van Defensie oordeelt op basis van de aangeleverde gegevens of het initiatief voor de persoonsgerichte kennisvergaring in het desbetreffende geval spoedeisend en gewichtig was met het oog op een veilig en doeltreffend optreden van eenheden of onderdelen van de krijgsmacht in de relevante operationele omgeving. Indien de minister tot het oordeel komt dat het initiatief in de specifieke omstandigheden gerechtvaardigd is geeft deze goedkeuring voor de persoonsgerichte kennisvergaring. Daarbij kan de minister toestaan dat het goedgekeurde initiatief voor maximaal dertig dagen wordt voortgezet.

Vierde lid

Nadat de termijn van voortzetting (van maximaal de dertig dagen) is verstreken mag de persoonsgerichte kennisvergaring uitsluitend plaatsvinden op grond van een aanwijzing. Het kan gaan om een omzetting van de goedkeuring in een aanwijzing, maar indien er omstandigheden zijn op grond waarvan de aanwijzing beperkter of breder moet zijn kan dat ook in de aanwijzing worden opgenomen. De aanwijzing kan in de praktijk ook gepaard gaan met een verzoek om goedkeuring.

Vijfde lid

De Minister van Defensie geeft met zijn goedkeuring aan dat het verwerken van persoonsgegevens ten behoeve de persoonsgerichte kennisvergaring noodzakelijk was. Indien de toestemming niet wordt verleend moet het verwerken van persoonsgegevens onmiddellijk stoppen. Aan het onthouden van goedkeuring kunnen verschillende gevolgen verbonden worden. Afhankelijk van de situatie kan de Minister van Defensie de passende gevolgen verbinden aan de reeds verzamelde persoonsgegevens.

Artikel 2.9 (afstemming MIVD persoonsgerichte kennisvergaring)

Eerste lid

De krijgsmacht en de MIVD versterken elkaar waar wettelijk toegestaan in de taakuitvoering. Dat betekent dat de krijgsmacht voor zover mogelijk gebruik maakt van de inlichtingen die zij van de MIVD mag ontvangen bij de persoonsgerichte kennisvergaring. Tegelijkertijd heeft de krijgsmacht op grond van artikel 4.9 van de wet de bevoegdheid om in bepaalde gevallen zelf persoonsgegevens te verzamelen. Daarbij is het niet uitgesloten dat in voorkomende gevallen zowel door de krijgsmacht als de MIVD kennis wordt vergaard omtrent dezelfde specifieke persoon, daarom dient hierover afstemming plaats te vinden. Dit heeft tot doel te voorkomen dat er conflicterende handelingen ontstaan, dat de beschikbare middelen op een efficiënte wijze worden ingezet en dat er een dubbele inbreuk op het recht op de persoonlijke levenssfeer plaatsvindt.

De MIVD wordt geïnformeerd over de kennisvergaring over een persoon waarover een ernstig vermoeden bestaat dat deze een gevaar vormt voor de veiligheid van de krijgsmacht of de militaire taakuitoefening van de betrokken eenheden. Op basis van die informatie kan de MIVD kenbaar maken dat het onwenselijk is dat de kennisvergaring wordt voortgezet, bijvoorbeeld omdat er reeds een onderzoek loopt over een bepaalde persoon.

De verplichting om de MIVD te informeren bestaat alleen voor de personen die een gevaar vormen voor de veiligheid van de krijgsmacht (personen in de zin van artikel 4.9, vierde lid,

onderdeel a, Wodg). De verplichting ziet niet op de andere categorieën van personen in artikel 4.9, vierde lid, van de Wet op defensiegereedheid omdat deze personen niet snel onderdeel vormen van de onderzoeken door de MIVD.

Tweede lid

Op basis van kennisgeving over de persoonsgerichte kennisvergaring kan er tussen de krijgsmacht en de MIVD een overleg plaatsvinden waarin wordt afgestemd over de persoonsgerichte kennisvergaring over personen die een gevaar vormen voor de veiligheid van de krijgsmacht.

Derde lid

De kennisgeving kan ook aanleiding zijn voor de MIVD om de Minister van Defensie te adviseren over de voortzetting van de persoonsgerichte kennisvergaring door de krijgsmacht. Indien de MIVD op basis van de kennisgeving hiervoor gronden ziet wordt kan het hoofd van de MIVD bij de Minister van Defensie aangeven dat de kennisvergaring door de krijgsmacht over bepaalde personen onwenselijk is vanuit de taakuitvoering door de MIVD.

Vierde lid

Een belangrijk onderdeel van de samenwerking tussen de krijgsmacht en de diensten is de vertrouwelijkheid en gevoelige aard van de informatie. Het is onwenselijk dat de krijgsmacht – ook al is dat binnen de goede uitvoering van de wet en gebaseerd op de gronden uit artikel 4.13 Wodg – gegevens door verstrekt aan derde partijen die een dienst zelf niet zou verstrekken. Op grond daarvan is vereist dat de dienst van wie Defensie gegevens heeft ontvangen voorafgaand aan een beoogde doorverstrekking goedkeuring geeft voor die verstrekking. Die toestemming kan ook structureel verleend worden voor bepaalde gegevens indien daar vooraf afspraken over gemaakt worden.

Artikel 2.10 (gegevensverstrekking aan personen en instanties)

Dit artikel creëert een grondslag voor de verstrekking van persoonsgegevens overeenkomstig artikel 4.13, vierde lid, Wodg. In aanvulling op de personen en instanties genoemd in artikel 4.13, eerste lid, Wodg kunnen op grond van deze bepaling persoonsgegevens verstrekt worden aan de Kustwacht Nederland en de Kustwacht Caribisch Gebied (het Caribisch deel van het Koninkrijk der Nederlanden).

De Kustwacht Nederland en de Kustwacht Caribisch Gebied leveren een belangrijke bijdrage aan het verantwoord gebruik van en de veiligheid van de wateren waartoe zij op grond van hun respectievelijke wetgeving bevoegd zijn taken uit te voeren.[32] Het gaat hier onder meer om de Noordzee en Waddenzee[33] respectievelijk de binnenwateren en territoriale zee van de Caribische

[32] Artikel 2, tweede lid, Regeling organisatie Kustwacht Nederland en Artikel 2 Rijkswet Kustwacht voor Aruba, Curaçao en Sint Maarten alsmede voor de openbare lichamen Bonaire, Sint Eustatius en Saba.
[33] Artikel 5 Regeling organisatie Kustwacht Nederland.

landen van het Koninkrijk en de openbare lichamen Bonaire, Sint Eustatius en Saba (delen van de Caraïbische Zee).[34]

De taken van de Kustwacht en de krijgsmacht hebben op dit gebied raakvlakken in de zin dat beiden actief zijn in het beschermen van de veiligheid op het water. De krijgsmacht richt zich binnen de territoriale wateren op dreigingen van statelijke actoren. Sinds 2023 heeft de krijgsmacht de taak om bij te dragen aan het beeld van dreigingsactoren en factoren op de Noordzee en in afstemming met NAVO bondgenoten en Europese partners zorg te dragen voor de begeleiding van niet-NAVO en niet-partner eenheden door het Nederlandse deel van de Noordzee.[35] De Kustwacht Nederland is een rechtshandhavingsorganisatie en onder meer verantwoordelijk voor de handhaving van regels betreffende scheepvaart, milieu, criminaliteit en visserij en het bewaken van de maritieme veiligheid, waarbij de focus met name is gericht op niet-statelijke actoren.

Vanuit haar grondwettelijke taken, in het bijzonder betreffende de informatiepositie en bewaken en beveiligen, heeft de krijgsmacht de beschikking over gegevens op het gebied van dreigingen of gevaren op of onder het water. Het is daarbij niet uitgesloten dat het om persoonsgegevens gaat. Bijvoorbeeld wanneer informatie over een verdacht schip gedeeld wordt, kan die informatie mogelijk gegevens bevatten die herleidbaar zijn tot een persoon. Zoals in § 3 toegelicht draagt het verstrekken van die gegevens bij aan het versterken van de maritieme veiligheid op het water en de handelingsperspectieven binnen de rechtshandhavingsketen.

Artikel 3.1 (toepassingsbereik)

Eerste lid

Deze bepaling beperkt de reikwijdte van hoofdstuk 3 van dit besluit. De bepalingen in hoofdstuk 3 geven uitvoering aan artikel 3, vierde lid, UAVG en betreffen de regels over de verwerking van persoonsgegevens bij de inzet of het ter beschikking stellen van de krijgsmacht.

Wanneer de regering besluit tot het inzetten of ter beschikking stellen van de krijgsmacht, dan geeft de krijgsmacht uitvoering aan een taak van algemeen belang: de taken opgenomen in artikel 97, eerste lid, van de Grondwet. Bij de uitvoering van die taken kan het noodzakelijk zijn om persoonsgegevens te verwerken. In de UAVG is daaromtrent reeds bepaald dat de AVG en UAVG, met uitzondering van de artikelen 9 en 10, hoofdstuk III en de artikelen 33, 34 en 36 AVG en de artikelen 22 tot en met 33 UAVG, van overeenkomstige toepassing zijn op die verwerkingen.[36]

Dit hoofdstuk is niet van toepassing indien de inzet van de krijgsmacht op andere specifieke grondslagen is gebaseerd. Het gaat daarbij om inzet van de krijgsmacht in het kader van nationale taken onder civiel gezag, bijvoorbeeld op grond van bijstand, steunverlening of structurele nationale taken.[37] Het regime voor gegevensverwerking wordt in dat geval bepaald

[34] Artikel 3 Rijkswet Kustwacht voor Aruba, Curaçao en Sint Maarten alsmede voor de openbare lichamen Bonaire, Sint Eustatius en Saba.
[35] *Kamerstukken II* 2022/23, 33 450, nr. 122.
[36] Artikel 3, derde lid, onderdeel b, UAVG.
[37] Bijvoorbeeld op grond van de Politiewet 2012, de Wet veiligheidsregio's of de Regeling militaire steunverlening in het openbaar belang.

door de kaders van gegevensverwerking die horen bij de grondslag waarop de krijgsmacht in dat geval wordt ingezet.

Tweede lid

Deze bepaling geeft een nadere duiding van het doel waarvoor persoonsgegevens verwerkt mogen worden bij de uitvoering van de taken uit artikel 97, eerste lid, van de Grondwet. In samenhang met artikel 97, eerste lid, van de Grondwet en artikel 3, derde lid, onderdeel b, UAVG vormt dit de grondslag voor het verwerken van persoonsgegevens bij inzet van de krijgsmacht. Het ter beschikking stellen van de krijgsmacht betreft militairen ter beschikking stellen ten behoeve van een vredesmacht of andere maatregel van een internationaal verband, zoals de VN of NAVO.[38] Het gaat daarbij om maatregelen ter handhaving of bevordering van de internationale rechtsorde. Bij het ter beschikking stellen van de krijgsmacht wordt in beginsel gehandeld onder de verantwoordelijkheid van het internationale verband en vindt de verwerking van persoonsgegevens op grond daarvan plaats.

De verwerking dient noodzakelijk te zijn voor een veilige en doeltreffende inzet van de krijgsmacht in de relevante operationele omgeving. Daaronder valt ook de bescherming van alle eenheden die in internationaal verband deelnemen aan een specifieke militaire operatie (de troepenmacht). Voor een veilige en doeltreffende operationele inzet van de krijgsmacht is vereist dat de krijgsmacht voortdurend een beeld heeft van de operationele omgeving om te weten wat de kansen en risico’s zijn voor de operatie. Enerzijds gaat het om de risico’s voor de eigen eenheden en het doel om deze veilig in te zetten. Anderzijds gaat het er om de vijand doeltreffend te raken en proportioneel te handelen. Het is in de operationele omgeving van essentieel belang om een onderscheid te maken tussen burgers en militairen of andere gevaarlijke actoren en tussen civiele infrastructuur en militaire doelwitten. Hiermee kan bewerkstelligd worden dat alleen militaire doelen geraakt worden.

Het mandaat voor de inzet geeft een inkadering van het doel van een veilige en doeltreffende inzet van de krijgsmacht in de relevante operationele omgeving. Het kan hier gaan om een internationaal mandaat op basis waarvan de krijgsmacht wordt ingezet of een nationaal mandaat. Dit is het politieke besluit tot en afbakening van het militair optreden, waarmee ook de reikwijdte van de bevoegdheden om gegevens te verwerken worden bepaald. Wanneer bijvoorbeeld een resolutie van de Veiligheidsraad van de Verenigde Naties (VN-Veiligheidsraad) militaire interventie autoriseert voor een bepaald doel, dan moet de verwerking van persoonsgegevens ook beperkt blijven tot het doel waarvoor de autorisatie gegeven is. Het nationaal mandaat verduidelijkt dat de krijgsmacht ook door de regering ingezet kan worden zonder dat daarvoor een specifiek internationaalrechtelijk mandaat benodigd is. Dit kan bijvoorbeeld het geval zijn bij speciale operaties. Bij speciale operaties gaat het om bijzondere militaire operaties die worden gekenmerkt door grote politiek-militaire risico's en de noodzaak tot strikte geheimhouding.[39] Dit kan tot doel hebben om tijdig escalatie van sluimerende conflicten te kunnen signaleren en daarop indien wenselijk te handelen (‘early warning, early

[38] *Kamerstukken II* 1996/97, 25 367 (R 1593), nr. 3, p. 4.
[39] *Kamerstukken II* 1999/2000, 26 800 X, nr. 46.

action'). Naast speciale operaties kan bij inzet op grond van nationaal mandaat gedacht worden aan inzet van de krijgsmacht op de Noordzee.

De verwerking van persoonsgegevens van eigen personeel en van personeel van andere deelnemende landen aan een operatie is niet gebaseerd op de uitoefening van het mandaat. Om die reden is dit hoofdstuk ook niet van toepassing op eigen personeel of personeel van andere deelnemende landen aan de operatie of op de bedrijfsvoering. Hierop is de AVG onverkort van toepassing.

Artikel 3.2 (verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard)

Eerste lid

Biometrische en genetische gegevens zijn bijzondere categorieën van persoonsgegevens. De verwerking van deze gegevens moet in de eerste plaats noodzakelijk zijn voor een veilige en doeltreffende uitoefening van het internationale of nationale mandaat voor de inzet van de krijgsmacht. Binnen dat kader geldt dat deze gegevens alleen verwerkt mogen worden als dit noodzakelijk is voor het vaststellen en de verificatie van de identiteit van een persoon. Daarbij valt te denken aan het verwerken van biometrische gegevens die zijn verkregen van geïmproviseerde explosieven. Ook het gericht vergelijken van personen met een zogenaamde (biometrische) watchlist is in dit verband mogelijk indien de verwerkte persoonsgegevens bij het ontbreken van een match niet opgeslagen of direct verwijderd worden.

Tweede lid

De verwerking van genetische gegevens is een vergaande inbreuk op de persoonlijke levenssfeer en is daarom alleen toegestaan voor het vaststellen en de verificatie van de identiteit van een persoon en beperkt tot personen die verdacht worden van strafbare feiten die ofwel verband houden met een gewapend conflict ofwel gericht zijn tegen de veiligheid van de troepenmacht.

Derde lid

Met het derde lid worden regels gesteld over andere bijzondere categorieën van persoonsgegevens dan biometrische en genetische persoonsgegevens en over persoonsgegevens van strafrechtelijke aard. Voor deze persoonsgegevens geldt dat deze niet verwerkt mogen worden tenzij dit noodzakelijk is voor een veilige en doeltreffende uitoefening van het internationale of nationale mandaat voor de inzet van de krijgsmacht. Daarnaast is vereist dat deze persoonsgegevens enkel worden verwerkt in samenhang met andere 'gewone' gegevens over de natuurlijke persoon in kwestie en de verzamelde persoonsgegevens afdoende zijn beveiligd.

Hiermee wordt uitvoering gegeven aan het advies van de Afdeling advisering van de Raad van State zoals dit is aangekondigd in de memorie van toelichting op de Rijkswet betreffende goedkeuring van Conventie 108 en Conventie 108+.[40] Daarnaast wordt in lijn met artikel 6 van Conventie 108+ ook voorzien in regels betreffende persoonsgegevens van strafrechtelijke aard,

[40] *Kamerstukken II* 2023/24, 36 455 (R2188), nr. 3.

waarbij ervoor is gekozen om de bepaling zoveel mogelijk te laten aansluiten bij de bepaling over gereedstelling.

Artikel 3.3 (gegevensverstrekking)

Eerste lid

Aan de justitiële autoriteiten (politie, Koninklijke marechaussee en het openbaar ministerie) kunnen ten behoeve van het voorkomen, opsporen, onderzoeken en vervolgen van strafbare feiten gegevens worden verstrekt. Bij inzet gaat het daar bijvoorbeeld om het verstrekken van zogenaamde 'battlefield information' of 'battlefield evidence'. Hoewel het verzamelen van gegevens uit een conflictgebied ten behoeve van justitiële doeleinden het best uitgevoerd kan worden door gespecialiseerd personeel, kan andere informatie die verwerkt wordt tijdens militaire operaties ondersteunend zijn aan deze doeleinden. Daarom wordt de mogelijkheid om operationele gegevens te delen voor justitiële doeleinden hier opgenomen als verstrekkingsgrond. Die verstrekking zal niet plaatsvinden als de vertrouwelijkheid zich in dat specifieke geval zich tegen die verstrekking verzet. Het gaat hier bijvoorbeeld om kritieke informatie over bepaalde operaties of kwetsbaarheden binnen de krijgsmacht waarbij verstrekking in dat geval risico's met zich meebrengt. De vertrouwelijkheid kan zich in dit verband ook tijdelijk verzetten tegen die verstrekking.

Tweede lid

Operationele inlichtingenproducten zijn documenten met gewaardeerde informatie over de omgeving en de capaciteiten en intenties van actoren in het operatiegebied om dreigingen en mogelijkheden te onderkennen ten behoeve van het operationele besluitvormingsproces. In deze inlichtingenproducten zijn vaak persoonsgegevens opgenomen. Het verstrekken van deze operationele inlichtingenproducten is beperkt tot de deelnemende landen aan een operatie dan wel met een internationale organisatie die de operatie uitvoert. Het gaat bij deze beperkte verstrekking zowel om EU-lidstaten als derde landen in de zin van hoofdstuk V van de AVG. Deze verstrekking is essentieel voor het veilig en succesvol kunnen uitvoeren van de operatie. Over het algemeen is de hoeveelheid persoonsgegevens in deze producten beperkt.

Derde lid

Het delen van persoonsgegevens met andere deelnemende landen aan een operatie of internationale organisaties, bijvoorbeeld door toegang te verlenen tot lokale databases met persoonsgegevens van nagetrokken personen of biometrische gegevens, levert een meerwaarde op voor de effectiviteit van de operatie. Waar het tweede lid persoonsgegevens betreft die onderdeel zijn van de context van de beoordeling van de operationele situatie, gaat het in het derde lid om verzamelingen van – soms grote hoeveelheden – persoonsgegevens. Hoewel het delen van deze gegevens van belang is voor de effectiviteit van de operatie, rechtvaardigt het verstrekken van deze gegevens vanwege de aard en omvang een aanvullende waarborg. Aan de ontvanger kunnen alleen persoonsgegevens worden verstrekt onder de voorwaarde dat die gegevens alleen verwerkt worden voor het doel van de verstrekking en voor de duur van de

betreffende operatie.[41] Het gaat daarbij dus om de doelbinding en bewaartermijn van de gegevens die door de ontvangende partij nageleefd moet worden.

Deze waarborg geldt zowel voor de verstrekking aan deelnemende EU-lidstaten als derde landen in de zin van hoofdstuk V van de AVG.

Vierde lid

Voor zover het bij deze verstrekking om bondgenoten gaat die een derde land (land buiten de Europese Economische Ruimte) of internationale organisatie zijn in de zin van Hoofdstuk V van de AVG gelden aanvullende waarborgen. Het gaat hier om dezelfde waarborgen zoals die overeenkomstig artikel 4.13, derde lid, Wodg gelden voor de verstrekking van gegevens op grond van die wet.

Bij de verstrekking van persoonsgegevens dient een belangenafweging plaats te vinden tussen het belang van de verstrekking en het belang van de betrokkene en de belangen van het Koninkrijk, waaronder de betrekkingen van Nederland met andere landen en internationale organisaties. Als onderdeel van die belangenafweging dient afgewogen te worden of de fundamentele mensenrechten,[42] in het bijzonder het recht op leven en het recht op vrijheid, voldoende worden beschermd door de ontvanger.[43] Relevante factoren zijn daarbij de omgang van de ontvanger met overgedragen gegevens, indicaties dat gegevens worden gebruikt voor politieke vervolging of onmenselijke of vernederende behandeling of bestraffing en de mate waarin gegevens kunnen worden opgeëist in het derde land.

In het kader van de verstrekking aan derde landen zij vermeld dat het de voorkeur verdient om persoonsgegevens te verstrekken door middel van een bilateraal of multilateraal verdrag dan wel via een administratieve regeling (met afdwingbare en effectieve rechten van betrokkene) met goedkeuring van de Autoriteit persoonsgegevens.[44] In de praktijk blijkt de verstrekking op grond hiervan ingewikkeld, omdat internationale partners niet altijd welwillend staan tegenover een Europees verdrag met Europese juridische verplichtingen. De gegevensverstrekking vindt om die redenen, en in lijn met de richtsnoeren van de het Europees Comité voor gegevensbescherming (EDPB) plaats op grond van artikel 49, eerste lid, onderdeel d, AVG.[45] Als waarborg in het kader van een verstrekking op grond van artikel 49 AVG is het uitgangspunt dat hierover wel een regeling met waarborgen wordt overeengekomen met het desbetreffende land.

Artikel 3.4 (bewaartermijn)

Persoonsgegevens die voor een veilig en doeltreffend optreden van de krijgsmacht binnen het gestelde mandaat zijn verzameld kunnen bewaard worden, tenzij direct duidelijk is dat het bewaren van deze gegevens niet langer noodzakelijk is voor dit doel. Dit kan bijvoorbeeld het geval zijn zolang Nederland deelneemt aan een operatie. Na beëindiging van de Nederlandse

[41] Vgl. artikel 4.13, zesde lid, Wodg.
[42] In ieder geval de borging van mensenrechten uit de artikelen 1 tot en met 6 van het Handvest.
[43] Vgl. artikel 88, derde lid, Wiv 2017.
[44] Artikel 46, tweede lid, onderdeel a, en derde lid, onderdeel b, AVG.
[45] Europees Comité voor gegevensbescherming, *Richtsnoeren 2/2018 inzake afwijkingen op grond van artikel 49 van Verordening 2016/679*, mei 2018.

deelname zal in de regel het nationale of internationale mandaat en daarmee ook het doel voor de verwerking van deze gegevens door de krijgsmacht vervallen.

Hierop zijn echter uitzonderingen. Het doel van de verwerking kan in de weg staan aan het verwijderen van de persoonsgegevens na beëindiging van de Nederlandse deelname. Dit kan bijvoorbeeld het geval zijn bij persoonsgegevens van vastgenomen personen. Ook het feit dat deelname aan dezelfde operatie in de nabije toekomst is voorzien, kan bijvoorbeeld in de weg staan aan het verwijderen van de persoonsgegevens. Voor zover dat nog niet gebeurd is tijdens de uitvoering van de operatie kunnen gegevens gedeeld worden met andere deelnemende landen, mits voldaan is aan het bepaalde in artikel 3.3. Daarnaast kan op verzoek besloten worden om (delen van) de gegevens in geanonimiseerde vorm beschikbaar te stellen voor evaluatie- of instructiedoeleinden.

Het uitgangspunt is dat persoonsgegevens worden vernietigd wanneer deze niet of niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt. Op grond van andere wettelijke voorschriften, in het bijzonder de Archiefwet 1995, kan er een verplichting bestaan om gegevens, waarin zich persoonsgegevens kunnen bevinden, te bewaren. Om die reden worden in het proces persoonsgegevens eerst verwijderd. Hierbij wordt aangesloten bij het regime zoals dat is opgenomen in artikel 4.7, eerste lid, Wodg.

Artikel 3.5 (rechten van betrokkene)

Met deze bepaling wordt voorzien in een eigen regime van rechten van betrokkene, waarbij rekening wordt gehouden met de specifieke context waarin de gegevensverwerkingen bij inzet plaatsvindt. Hierbij wordt aangesloten bij het regime zoals dat ook op grond van de Wet op de defensiegereedheid geldt bij de gereedstelling.

Eerste lid

De Minister van Defensie heeft de verplichting om het publiek te informeren over de verwerkingen door de krijgsmacht in algemene zin. Deze bepaling wijkt deels af van artikel 4.14 Wodg, doordat er geen verplichting bestaat om kenbaar te maken waar en welke activiteit gedurende de inzet verricht wordt. Die afwijking is gelegen in het feit dat het kenbaar maken van deze informatie een direct gevaar oplevert voor de operatie en de veiligheid van de troepenmacht. Voor het overige dient de Minister van Defensie in algemene zin kenbaar te maken hoe een betrokkene in contact kan komen met Defensie om bijvoorbeeld een vraag te stellen of klacht in te dienen, voor welke doelen (op grond van dit hoofdstuk van dit besluit) gegevens verwerkt worden en welke rechten een betrokkene heeft.

Tweede en derde lid

Een betrokkene heeft het recht op kennisneming van de verwerkte persoonsgegevens van deze betrokkene voor een veilige en doeltreffende uitoefening van het internationale of nationale mandaat voor de inzet van de krijgsmacht. Op dit recht zijn de procedurele regels, het recht om een verklaring omtrent de gegevens te overleggen en de weigeringsgronden en beperkingen uit de artikelen 4.15 tot en met 4.17 van overeenkomstige toepassing.