DPIA
Wet op de defensiegereedheid (Wodg)

Versie	0.99 (a.d.h.v. Model DPIA Rijksdienst v3.0)
Rubricering	DEPARTEMENTAAL VERTROUWELIJK
Status	Vertrouwelijk en concept *(gebaseerd op Voorlopig ontwerp Wodg versie 2.2 van 04-03-2025)*
Datum	04-03-2025

Inhoudsopgave

Managementsamenvatting 3

A Beschrijving kenmerken gegevensverwerkingen 7

1. Voorstel 7

2. Persoonsgegevens 12

3. Gegevensverwerkingen 14

4. Technieken en methoden van de gegevensverwerkingen 18

5. Verwerkingsdoeleinden 19

6. Betrokken partijen 20

7. Belangen bij de gegevensverwerkingen 22

8. Verwerkingslocaties 24

9. Juridisch en beleidsmatig kader 26

10. Bewaartermijnen 30

B Beoordeling rechtmatigheid gegevensverwerkingen 31

11. Rechtsgrond 31

12. Bijzondere persoonsgegevens 32

13. Doelbinding 33

14. Noodzaak en evenredigheid 35

15. Rechten van betrokkenen 42

C Beschrijving en beoordeling risico's voor de betrokkenen 44

16. Risico's voor betrokkenen 44

D Maatregelen en restrisico's 46

17. Maatregelen 46

Ondertekening 51

Managementsamenvatting

Doel Wodg

De Wet op de defensiegereedheid (Wodg) creëert een wettelijk kader met als doel een daadwerkelijke en stelselmatige gereedheid van het militair vermogen, en afstemming van dit belang op andere belangen in een weerbare maatschappij.[1] Dit kader is van toepassing op zowel activiteiten van de krijgsmacht als op de bijdrage die de andere defensieonderdelen leveren. Het wetsvoorstel voorziet in een rechtsgrond voor de verwerking van persoonsgegevens in het kader van de uitvoering van de in het wetsvoorstel beschreven publieke taken. De Wodg verklaart de Algemene Verordening Gegevensbescherming (AVG) van overeenkomstige toepassing met een aantal specifieke uitzonderingen op de AVG en de Uitvoeringswet AVG (UAVG), zoals bepaald in artikel 4.4 van de Wodg.

Doel DPIA

Deze *Data Protection Impact Assessment* (DPIA) betreft een verplichte evaluatie van de verwerkingen van persoonsgegevens die voortvloeien uit het wetsvoorstel (artikel 35, eerste lid, AVG). Daarbij ligt de focus op verwerkingen van persoonsgegevens die, gelet op de aard, de omvang, de context en de doeleinden, waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen.

DPIA onderdelen

De DPIA volgt het Rijksmodel DPIA en draagt bij aan de integratie van de bescherming van persoonsgegevens in de belangenafweging en besluitvorming rond nieuwe wetgeving.[2] Het Rijksmodel DPIA houdt een viertal onderdelen aan:

A. Beschrijving van gegevensverwerkingen
B. Beoordeling rechtmatigheid gegevensverwerkingen
C. Beschrijving en beoordeling risico's voor de betrokkenen
D. Maatregelen en restrisico's

DPIA proces

De uitvoering van de DPIA begon in een vroeg stadium van het wetgevingsproces en is een dynamisch en iteratief proces. Daarbij is voortgebouwd op eerdere analyses, inzichten en bestaande juridische kaders,[3] en input van diverse stakeholders, waaronder juristen, beleidsmedewerkers, en operationele experts. Ten behoeve van de DPIA heeft afstemming plaatsgevonden met AVG-coördinatoren vanuit de Defensieonderdelen, de procesbegeleider Wodg, twee hoogleraren van de Nederlandse Defensieacademie (NLDA) en de FG-unit (via informele consultaties). Voorliggende versie van de DPIA kan naar aanleiding van vragen uit de internetconsultatie en aanvullende Algemene Maatregelen van Bestuur (AMvB's) worden herzien of aangevuld.

Gereedstellingsactiviteiten

Deze DPIA richt zich op de gereedstellingsactiviteiten die plaatsvinden binnen de informatieomgeving, waarbij duidelijk is dat binnen dit cluster

[1] Memorie van Toelichting (MvT), paragraaf 1.2, Voorlopig ontwerp Wodg, versie 2.1.
[2] Het Rijksmodel DPIA is niet volledig geëquipeerd voor het beoordelen van wet- en regelgeving en beleid. Er is een concept model Gegevensbeschermingstoets Wetgeving Rijk in ontwikkeling dat hier meer recht aan doet. Dit niet-vastgestelde model is gebruikt om het Rijksmodel aan te vullen en te verrijken.
[3] Zoals de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017), de rapporten 'Grondslag gezocht' van de commissie Brouwer, 'Tanden voor de Leeuw' van de NLDA, 'Nederland in een fragmenterende wereldorde' van de WRR en de beleidsvisie Informatiegestuurd Optreden (IGO).

persoonsgegevens (o.a. van Defensiepersoneel) worden verwerkt (H4 en H5 van de Wodg). De clusters inkoop (H6) en fysieke leefomgeving (H3) impliceren niet direct verwerkingen van persoonsgegevens. Als dit in de toekomst wel het geval blijkt te zijn, wordt zo nodig een aanvullende DPIA uitgevoerd. Voor het cluster informatieomgeving vindt een nadere specificatie plaats naar "geoefendheid en gereedheid"[4] (artikel 2.1 a-c), "informatiepositie" (artikel 2.1 d) en "bewaken en beveiligen" (artikel 2.1 e).

Het wetsvoorstel voorziet in maatregelen om de beschikbaarheid, integriteit en veiligheid van persoonsgegevens te waarborgen, waaronder toegangs- en verstrekkingsregimes. Aanvullende waarborgen zijn van toepassing bij de mogelijkheid voor incidentele vergaring van kennis over en het stelselmatig monitoren van personen (zie artikel 4.7, lid 3-7 en 4.8, lid 2-3) alsmede gegevensverstrekking(en) aan andere organisaties (artikel 4.12).

Proportionaliteit en subsidiariteit
Het wetsvoorstel biedt ruimte voor potentieel vergaande inbreuken op de persoonlijke levenssfeer. Deze inbreuken zijn mede afhankelijk van de wijze waarop daarvoor nadere regels worden gesteld bij AMvB en de wijze van uitvoering van de bevoegdheden. De juridische basis vormt de gedeeltelijke van overeenkomstige toepassing verklaring van de AVG en UAVG op de beoogde gegevensverwerkingen.

Het wetsvoorstel voorziet, als tegenhang voor de potentieel vergaande inbreuken, in een adequaat waarborgen- en toezichtstelsel, waaronder een eigen regime voor de rechten van betrokkenen (paragraaf 4.6) en er zijn nadere waarborgen ingericht voor de gerichte vergaring van kennis over specifieke personen (artikel 4.7, leden 3-7) en de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard (artikel 4.5).

Bovendien maakt de Wodg als wet in formele zin, gepaard met de Memorie van Toelichting (MvT), de afweging die ten grondslag ligt aan de inzet van de benodigde bevoegdheden transparanter en beter voorzienbaar voor betrokkenen dan de huidige werkwijze die gebaseerd is op een meer versnipperd juridisch kader. Tot slot zal conform de reguliere praktijk bij het daadwerkelijk gebruik van de bevoegdheden waar het wetsvoorstel een grondslag voor biedt per casus een toets op proportionaliteit en subsidiariteit moeten plaatsvinden.

Risico's en maatregelen
Bij de activiteiten en gegevensverwerkingen die voortvloeien uit het wetsvoorstel, zijn diverse risico's en maatregelen te identificeren. Deze zijn geformuleerd op een hoog abstractieniveau om een breed beeld te geven van de potentiële risico's met betrekking tot de rechten en vrijheden van individuen.

Risico's (H16)	**Pijler**	**Maatregelen (H17)**
Verlies van controle over persoonsgegevens door onduidelijke taakafbakening tussen (overheids-)instanties	Strategie	• Codificatie van taken en verantwoordelijkheden • (Beleids)afspraken en richtlijnen voor gegevensverstrekkingen • Communicatie(plannen) en betrokkenheid
	Mensen	• Gedrag en bewustwording

[4] De verwerkingen die op grond van artikel 2.1, tweede lid, onderdelen a tot en met c, in samenhang met artikel 4.6 plaats vinden, zien op de personele en materiële gereedheid alsmede de geoefendheid.

	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
Ongeautoriseerd gebruik van persoonsgegevens door gebrek aan regels (*scope creep*)	Strategie	• Besturing en verantwoordelijkheidstoewijzing • (Beleids)afspraken en gegevensverstrekking
	Mensen	• Gedrag en bewustwording
	Processen	• Begeleiding en ondersteuning • Evaluatie en incidentmanagement • Toezichthoudende processen
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Beveiliging • Anonimiseren en pseudonimiseren
Schade door inadequaat gegevensbeheer en gebrekkige beveiliging (inclusief incident management)	Mensen	• Gedrag en bewustwording
	Processen	• Begeleiding en ondersteuning • Evaluatie en incidentmanagement • Toezichthoudende processen
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Beveiliging • Anonimiseren en pseudonimiseren
Ongewenste profilering en discriminatie door geautomatiseerde systemen	Mensen	• Gedrag en bewustwording; datageletterdheid
	Processen	• Begeleiding en ondersteuning
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Ethisch gebruik, inzet van *Privacy Enhancing Technologies* (PET's), uitvoeren van audits • Anonimiseren en pseudonimiseren
Beperkte mogelijkheid tot uitoefening van rechten en toegang tot juridische bescherming door gebrek aan transparantie	Strategie	• Besturing en verantwoordelijkheidstoewijzing • (Beleids)afspraken en gegevensverstrekking
	Processen	• Begeleiding en ondersteuning
Verandering van gedrag door monitoring (*chilling effect*)	Strategie	• Communicatie(plannen) en betrokkenheid
	Mensen	• Gedrag en bewustwording
Te ruime verwerking van persoonsgegevens in het kader van de enquête	Strategie	• Besturing en verantwoordelijkheidstoewijzing • Beleidsafspraken en richtlijnen • Communicatie en betrokkenheid
	Mensen	• Gedrag en bewustwording
	Processen	• Begeleiding en ondersteuning • Evaluatie en incidentmanagement
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Anonimiseren en pseudonomiseren • Beveiliging

Bij verdere toetsing en evaluatie is aandacht nodig voor uitvoeringsrisico's en daadwerkelijke effectiviteit van de in het wetsvoorstel opgenomen waarborgen. Uitdagingen kunnen voortkomen uit een tekort aan capaciteit (kwantitatief en kwalitatief), beperkte prioritering en knelpunten voortkomend uit de huidige

volwassenheidsniveaus op het gebied van datamanagement, compliance- en privacy-processen. Hiertoe dienen diverse onderdelen nauw samen te werken, waarbij de operatie, IT, beleids- en privacyfuncties een belangrijke rol vervullen. De betreffende organisatieonderdelen binnen de defensieorganisatie dienen hiervoor te worden versterkt.

A Beschrijving kenmerken gegevensverwerkingen

1. Voorstel

De Wet op de Defensiegereedheid (Wodg) is ontworpen om de krijgsmacht en de defensieonderdelen effectief voor te bereiden op actuele en toekomstige dreigingen, met een focus op activiteiten (incl. verwerkingen van persoonsgegevens) in zowel de fysieke, cognitieve als de virtuele dimensies van de operationele omgeving.

Het wetsvoorstel codificeert de kaders voor de gereedstellingsactiviteiten als onderdeel van de publieke taken van Defensie. Deze *Data Protection Impact Assessment* (DPIA) richt zich op de gereedstellingsactiviteiten die plaatsvinden binnen het cluster van informatieomgeving (H4) en personeel (H5). Bij deze clusters is helder dat persoonsgegevens worden verwerkt. Uit de kaders voor de fysieke leefomgeving (H3) en inkoop (H6) volgen niet direct gegevensverwerkingen. Wanneer dit in het vervolg wel het geval blijkt te zijn, dan wordt daarvoor zo nodig een aanvullende DPIA uitgevoerd. De informatieomgeving is relevant in vrijwel alle (categorieën) gereedstellingsactiviteiten die worden gespecificeerd in artikel 2.1 van de Wodg. Concreter betreft dat activiteiten in het kader van de volgende drie taakgebieden: "geoefendheid en gereedheid"[5] (artikel 2.1 lid 2a-c), "informatiepositie" (artikel 2.1 lid 2d) en "bewaken en beveiligen" (artikel 2.1 lid 2e).

Probleemstelling
Zoals omschreven in de eerste paragraaf van de Memorie van Toelichting (MvT) is de aanleiding voor de Wodg de toenemende mondiale instabiliteit, gekenmerkt door een hogere frequentie en intensiteit van conflicten nabij Europa, en de opkomst van hybride dreigingen en oorlogsvoering.[6] Defensie moet voorbereid zijn op grootschalige militaire conflicten in het NAVO-verdragsgebied, zoals benadrukt in de Defensienota 2024[7] en de eerste formele toespraak van Mark Rutte als de secretaris-generaal van de NAVO.[8]

Het bestaande juridische raamwerk ten behoeve van de doelstellingen en taken van Defensie is verouderd en niet toereikend om de moderne eisen van technologie en informatiegestuurd optreden in hybride conflicten en multi-domein operaties te ondersteunen, zoals benadrukt in rapporten zoals 'Grondslag gezocht'[9] (Commissie Brouwer), 'Tanden voor de Leeuw'[10] (NLDA), 'Nederland in een fragmenterende wereldorde' (WRR)[11] en 'Hybride dreigingen

[5] De verwerkingen die op grond van artikel 2.1, tweede lid, onderdelen a tot en met c, in samenhang met artikel 4.6 plaats vinden, zien op de personele en materiële gereedheid alsmede de geoefendheid.
[6] Wijk, Rob de., Frank Bekkers en Tim Sweijs, "Hybride Dreigingen en Hybride Oorlog: Consequenties voor de Koninklijke Landmacht." The Hague Centre for Strategic Studies, HCSS Security (2020).
[7] Ministerie van Defensie, Defensienota 2024, p. 22.
[8] In zijn eerste formele toespraak als secretaris-generaal van de NAVO sprak Rutte uit: we zijn niet in oorlog, "maar er is zeker geen vrede" en "We zijn niet klaar voor wat ons over vier tot vijf jaar te wachten staat".
[9] Onderzoekscommissie Land Information Manoeuvre Centre (LIMC), Grondslag gezocht, December 2022. Zie ook: Kamerstukken II, 2022/23, 32761, nr. 258.
[10] Ducheine, Paul, Peter Pijpers, Marten Zwanenburg, Rapport Tanden voor de Leeuw, Een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving, (NLDA-WSRC, 4-4-2024). Aangeboden via Kamerstukken II, 2024-25, 33763, nr. 158.
[11] Wetenschappelijke Raad voor Regeringsbeleid, Nederland in een fragmenterende wereldorde (WRR, rapport nr. 109), 2024.

en maatschappelijke weerbaarheid' (AIV).[12] Defensie heeft in een aantal gevallen wel publieke taken in het informatiedomein, maar die zijn slechts uitgewerkt in een wet in materiële zin, en voor het overige ontbreekt het aan een wettelijke grondslag om rechtmatig persoonsgegevens te mogen verwerken.[13]

Doel van de Wodg
De Wodg heeft tot doel een wettelijk kader voor het tijdig gereedstellen van de krijgsmacht onder de verantwoordelijkheid van de minister van Defensie te scheppen. Zowel voor activiteiten van de krijgsmacht zelf en door ondersteunende activiteiten van andere onderdelen van het ministerie van Defensie. Het doel van de toepassing van dit kader is een daadwerkelijke en stelselmatige gereedheid van het militair vermogen, en afstemming van dit belang met andere belangen in een weerbare maatschappij.[14]

De Wodg werkt de doelomschrijving uit in gereedstellingsactiviteiten. Zoals gesteld focust deze DPIA zich op de gereedstellingsactiviteiten die plaatsvinden in de context van informatieomgeving en personeel. Voor het cluster informatieomgeving vindt een nadere specificatie plaats naar de taakgebieden "geoefendheid" (artikel 2.1 lid 2a en c), "informatiepositie" (artikel 2.1 lid 2d) en "bewaken en beveiligen" (artikel 2.1 lid 2e). Voor het personeel vindt een nadere specificatie plaats naar gezondheid en de monitoring hiervan (artikel 7.2 en 7.3).

De DPIA sluit aan bij eerdere analyses en volgt voornoemde specificaties, omdat de taakgebieden (grotendeels) eigen kenmerken hebben als het gaat om de verwerking van persoonsgegevens:

1. **Geoefendheid (opleiden, trainen en oefenen)[15]**
   Het voorbereiden, onderhouden en verbeteren van de geoefendheid van defensieonderdelen. Persoonsgegevens worden verwerkt in het proces van opleiden, trainen en oefenen voor het produceren van kennis, het ontwerpen en ontwikkelen van opleidingen en trainingen, het verzorgen van opleidings- en trainingsondersteuning (incl. monitoren en begeleiden van personeel binnen en buiten deze activiteiten). Het verwerken van persoonsgegevens is op zich niet altijd het doel, maar onvermijdelijk onderdeel van de informatie die in dit kader wordt verwerkt, zoals bijvoorbeeld bij bronvermeldingen, of bij het verwerken van data van

[12] Adviesraad Internationale Vraagstukken, "Hybride dreigingen en maatschappelijke weerbaarheid." (AIV-advies 126), 2024. Zie ook de kabinetsreactie op het AIV-advies (Kamerstuk 30 821, nr. 250).
[13] EIFFEL B.V., Onderzoek AVG – Ministerie van Defensie, juli 2022, p. 23.
[14] MvT, paragraaf 1.2, Voorlopig ontwerp Wodg, versie 2.1.
[15] Artikel 2.1, tweede lid, onder a, behandelt het voorbereiden, onderhouden en verbeteren van de geoefendheid van defensieonderdelen, wat aansluit bij het trainen en opleiden. Dit omvat activiteiten die nodig zijn voor het gereedstellen van het militaire vermogen, wat het plannen en uitvoeren van oefeningen kan inhouden. De begrippen opleiden, individueel trainen, collectief trainen, oefenen zijn als volgt gedefinieerd:
- Opleiden: het (initieel) aanleren van kennis, vaardigheden en houdingsaspecten (attitude) benodigd voor het uitvoeren van de opgedragen taak of (toekomstige) functie (niveau I).
- Individueel trainen: het (individueel) op peil houden en verdiepen van kennis, vaardigheden en houdingsaspecten (attitude), benodigd voor het uitvoeren van de opgedragen taak (niveau I).
- Trainen: het op peil houden en doorontwikkelen van kennis, vaardigheden en houdingsaspecten door eenheden benodigd voor het uitvoeren van hun taken (niveau II+).
- Oefenen: het in een gesimuleerde operationele situatie in de praktijk brengen van kennis, vaardigheden en houdingsaspecten met als doel de bedrevenheid in het plannen, voorbereiden en uitvoeren van de toegewezen operationele taken te onderhouden, te vergroten en te evalueren.

openbare online bronnen en bij oefeningen in de openbare ruimte met bijvoorbeeld onbemenste systemen met sensoren.

2. **Informatiepositie (omgevingsbeeld)[16]**
   Het vergaren van kennis over relevante operationele omgevingen en het vormen van een omgevingsbeeld, inclusief het analyseren en duiden daarvan, om onder andere bedreigingen te identificeren en af te schrikken. Persoonsgegevens kunnen worden geanalyseerd met technische hulpmiddelen voor monitoring en inzicht.

3. **Bewaken en beveiligen (incl. force protection)[17]**
   Het waarborgen van de veiligheid van militaire objecten, aangewezen krachtens de Rijkswet geweldgebruik bewakers militaire objecten, met aanvullende ruimte (t.o.v. de huidige Rijkswet) voor de beveiliging van de digitale infrastructuur en data. Persoonsgegevens worden verwerkt om fysieke en digitale beveiliging te garanderen zoals door het verzamelen en monitoren van *Cyber Threat Intelligence* (CTI) van Sensor, Wapen- en Communicatiesystemen (SEWACO). Het verzamelen van contra-inlichtingen valt buiten de scope van bewaken en beveiligen in deze DPIA, gelet op het feit dat dit een onderdeel van de taakstelling van de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) is.

4. **Personeel**
   Om de inzetbaarheid van militairen te waarborgen en hun gezondheid te beschermen worden bijzondere persoonsgegevens verwerkt in verband met de monitoring van hun gezondheid. Zo worden bijvoorbeeld bijzondere persoonsgegevens verwerkt in het kader van het uitvoeren van de aanstellingskeuring van specifieke (militaire) functies en epidemiologisch onderzoek. Daarnaast worden Nederlanders in de leeftijd tussen 17 en 27 jaar opgeroepen een enquête ten aanzien van hun interesse en geschiktheid voor Defensie in te vullen. Niet valt uit te sluiten dat persoonsgegevens over de gezondheid worden verwerkt.

Opties en keuze voor wetgeving

De Wodg moet mede gezien worden in verhouding tot aanpalende wetgeving zoals de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) en beleidsinitiatieven, zoals het Nationaal Programma Ruimte voor Defensie[18]. Verder is het een vervolg op de Beleidsvisie Informatiegestuurd Optreden (IGO)[19], ondersteund door de Defensie Strategie Data Science en AI 2023-2027. Het cluster 'informatieomgeving' in de Wodg past in de context van IGO. De Beleidsvisie IGO legde het fundament voor de operationalisering van IGO. Dit houdt in dat Defensie in staat moet zijn om:

1. (Informatie) sneller de juiste informatie te verzamelen en analyseren teneinde de situatie beter te begrijpen, zodat
2. (Gestuurd) snellere en betere besluiten genomen kunnen worden, om

[16] Artikel 4.7 en 4.8 gaan over het vergaren van kennis en het verkrijgen van een operationeel beeld van de omgeving. Dit omvat het verzamelen en verwerken van persoonsgegevens om de operationele omgeving te analyseren en te monitoren, wat overeenkomt met het verkrijgen van een gedetailleerd omgevingsbeeld.
[17] Dit is een randvoorwaarde om inzetgereed te zijn. Bij *force protection* is het primaire doel van beschermen behoud van vrijheid van handelen, zodat een succesvolle uitvoering van de opdracht mogelijk blijft. De functie bescherming omvat alle activiteiten (zowel verdediging (*defense*), als beveiliging (*security*) als bedrijfsveiligheid (*safety*), gericht op het voorkomen van ongewenste effecten op de eigen troepenmacht; daarbij worden risico's beperkt en zo mogelijk geneutraliseerd.
[18] Het Nationaal Programma Ruimte voor Defensie (NPRD), https://www.defensie.nl/onderwerpen/ruimte-voor-defensie hangt samen met de Nota Ruimte https://www.denationaleomgevingsvisie.nl/nota+ruimte/default.aspx.
[19] *Kamerstukken II*, 2022-23, 36 124, nr. 35.

3. (Optreden) met de beschikbare (militaire) middelen de gewenste effecten te bereiken.

Informatie dient als doel, middel en effector. Informatie wordt gebruikt voor voorspelling (*forecasting*), beeldvorming (*insight*) en oordeelsvorming (*foresight*), ter ondersteuning van commandovoering en voor het bereiken van effecten in de fysieke, cognitieve en virtuele dimensies.

De voorgeschiedenis van juridische en beleidsmatige kaders en adviezen vormt een belangrijke basis voor het wetsvoorstel en deze DPIA; de belangen en risico's die in eerdere analyses zijn geïdentificeerd en beoordeeld, zijn ook relevant voor deze beoordeling.

Voorafgaand aan de ontwikkeling van de Wodg zijn verschillende strategieën overwogen, zoals het verbeteren van de bestaande kaders en het ontwikkelen van tijdelijke organisatorische maatregelen.

Echter, deze opties bieden geen structurele oplossing voor het verzekeren van een daadwerkelijke en stelselmatige gereedheid van het militair vermogen van de krijgsmacht in een weerbare maatschappij. Het leidde tot de constatering dat het huidige juridische kader knelpunten oplevert bij de gereedstelling van de krijgsmacht voor het beschermen van het eigen en bondgenootschappelijk grondgebied en het effectief en geloofwaardig afschrikken.[20] De Wodg beoogt een juridisch fundament voor zowel huidige als toekomstige uitdagingen te bieden. Het wetsvoorstel wordt ondersteund door adviezen en onderzoeksrapporten van de commissie Brouwer[21], NLDA[22], WRR[23] en de AIV.[24]

Belanghebbenden

De Wodg heeft implicaties voor verschillende belanghebbenden, zoals:

- De Minister van Defensie: als verwerkingsverantwoordelijke aangewezen voor de in het wetsvoorstel omschreven taakgebieden.
- Defensieambtenaren (beroepsmilitairen, reservisten en burgers): voor effectief opleiden, trainen en oefenen, het vergaren van kennis voor de informatiepositie en veiligheid.
- Commandant: de functionaris als bedoeld in Besluit toedeling uitvoerende personele bevoegdheden Defensie 2021[25]. De commandant geeft leiding in de vorm van opdrachten of aanwijzingen, coördineert activiteiten en motiveert gelijktijdig zijn mensen door de persoonlijke wijze van optreden.
- NAVO-bondgenoten en EU-partners: zij rekenen op Nederland voor een bijdrage aan de collectieve verdediging en afschrikking, zoals bepaald in internationale verdragen.
- Burgers: zij hebben belang bij de bescherming van hun veiligheid, vrijheid en privacy. Het gaat om afwegingen tussen individuele rechten en waarden die aan het fundament liggen van onze samenleving en rechtsstaat.

[20] MvT, paragraaf 1.2, Voorlopig ontwerp Wodg, versie 2.1.
[21] 'Grondslag gezocht' Grondslag gezocht - Onderzoekscommissie Land Information Manoeuvre Centre (LIMC) van de commissie Brouwer (https://www.rijksoverheid.nl/documenten/rapporten/2023/01/13/rapport-onderzoekscommissie-brouwer-naar-het-land-information-manoeuvre-centre-limc)
[22] Ducheine, Paul, Peter Pijpers, Marten Zwanenburg, Rapport Tanden voor de Leeuw, Een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving, (NLDA-WSRC, 4-4-2024). Aangeboden via Kamerstukken II, 2024-25, 33763, nr. 158
[23] Wetenschappelijke Raad voor Regeringsbeleid, Nederland in een fragmenterende wereldorde (WRR, rapport nr. 109), 2024.
[24] Adviesraad Internationale Vraagstukken, "Hybride dreigingen en maatschappelijke weerbaarheid." (AIV-advies 126), 2024. Zie ook de kabinetsreactie op het AIV-advies (Kamerstuk 30 821, nr. 250).
[25] *Command*: The authority vested in a member of the armed forces for the direction, coordination, and control of military forces. NATO Agreed 2019-02-25.

- Nederlanders tussen de 17 en 27 jaar die een enquête ontvangen ten aanzien van hun interesse om bij Defensie te werken.

Specifieke uitzonderingen (U)AVG
In het wetsvoorstel wordt de AVG van overeenkomstige toepassing verklaard met een aantal specifieke uitzonderingen op de AVG en de Uitvoeringswet AVG (UAVG), zoals bepaald in artikel 4.4 van de Wodg. Het betreft een doorbrekingsgrond voor het verwerkingsverbod van bijzondere- en strafrechtelijke persoonsgegevens (artikel 6 van Conventie 108+), de beperking van rechten van betrokkenen (hoofdstuk III), melden van een inbreuk in verband met persoonsgegevens (artikel 33, 34 AVG) en voorafgaande raadpleging (artikel 36 AVG) en de artikelen 22 tot en met 33 UAVG.

2. Persoonsgegevens

Uit de Wodg zullen diverse activiteiten en verwerkingen van persoonsgegevens voortvloeien. Gezien het abstractieniveau van het wetsvoorstel en de aankondiging van verdere uitwerkingen in Algemene Maatregelen van Bestuur (AMvB's) bevat dit hoofdstuk voorbeelden van het type persoonsgegevens die naar huidig inzicht verwerkt worden. Hieronder zijn voorbeelden gegroepeerd in gereedstellingsactiviteiten in de informatieomgeving, gevolgd door personeel, zoals vervat in de aangeduide wetsartikelen in de Wodg.

Geoefendheid en Gereedheid (artikel 4.6)
Tijdens de uitvoering van gereedstellingsactiviteiten worden persoonsgegevens van defensieambtenaren en mogelijk ook van burgers verwerkt ter voorbereiding, training en verbetering van geoefendheid. Deze activiteiten omvatten het gebruik van sensoren en monitoringtechnologieën:

- **Gewone persoonsgegevens:** Namen, adressen, woonplaatsen, rangen/schalen en functies van defensiepersoneel.
- **Gevoelige persoonsgegevens:** Fysieke gegevens (geslacht, leeftijd), locatiegegevens (operationele gegevens) en gedragsinformatie verzameld tijdens oefeningen.[26]
- **Bijzondere persoonsgegevens:** Biometrische gegevens en gezondheidsinformatie indien relevant voor specifieke trainingen van militairen.[27]
    - Voor gereedstellingsactiviteiten in het kader van de opleiding, training en oefening ('geoefendheid') is het verwerken van persoonsgegevens op zich niet het doel, maar doorgaans onvermijdelijk onderdeel van de informatie die in dit kader wordt verwerkt. Deze informatie zal doorgaans terstond worden verwijderd.

Informatiepositie (artikelen 4.7, 4.8)
Defensie verzamelt persoonsgegevens om inzicht te krijgen in en zich voor te bereiden op de operationele omgeving. Dit omvat:

- **Gewone persoonsgegevens:** informatie van personen afkomstig uit openbare bronnen, zoals namen, contactgegevens, functie en operationele rollen, camerabeelden, kentekens.
- **Gevoelige persoonsgegevens:** locatiegegevens, digitale identificatiegegevens (zoals IP-adressen), gegevens over bewegingen en activiteiten in operationele gebieden, verkregen via monitoring en analyse.
- **Bijzondere persoonsgegevens**: biometrische gegevens (audio- en videomateriaal), inclusief openbare uitingen op bv. sociale media, nieuwskanalen, internetfora, 'discours', etc.

[26] Om na te gaan wat bijdraagt aan duurzame inzetbaarheid van militairen, worden bijvoorbeeld tijdens 'opleiden, trainen en oefenen' vitale functies zoals een hartslag, ademhaling en lichaamstemperatuur bijgehouden om prestaties te optimaliseren en gezondheidsschade te voorkomen in normale, verzwaarde en extreme omstandigheden. Draagbare sensortechnologie en de analyse van biometrische gegevens kan gebruikt worden om de fysieke belasting op het menselijk lichaam te monitoren en te gebruiken om veilig en verantwoord op te leiden, te trainen en te oefenen.
[27] Op camerabeelden van personen zijn de fysieke kenmerken van die personen zichtbaar. Zo is bijvoorbeeld zichtbaar of iemand een bril draagt (wat iets zegt over zijn visuele gezondheid) of een hoofddoek (wat iets kan zeggen over godsdienstige overtuiging). Tevens kan iemands ras van de camerabeelden worden afgeleid. De Autoriteit Persoonsgegevens beschouwt camerabeelden van een persoon niet als bijzondere persoonsgegevens als de verwerking niet specifiek gericht is op het verwerken van bijzondere persoonsgegevens of op het maken van onderscheid op grond van een bijzonder persoonsgegeven. Echter, indien de verwerking van camerabeelden gericht is op identificatie, kunnen deze beelden wel als bijzonder persoonsgegeven worden aangemerkt.

Bewaken en beveiligen: beveiliging van digitale infrastructuur (artikelen 4.9 en 4.10)
Voor de beveiliging van netwerken en informatiesystemen van Defensie worden activiteiten uitgevoerd en persoonsgegevens verwerkt, met als doel dreigingen te ontdekken en te reageren op cyberincidenten:

- **Gewone persoonsgegevens:** namen, functie en operationele rollen, camerabeelden, IP-adressen, gebruikersnamen, en netwerklogboeken die betrokken zijn bij cyberbeveiligingsmonitoring.
- **Gevoelige persoonsgegevens:** activiteitenlogboeken die gedragsgegevens bevatten en real-time monitoring van netwerkgebruik omvatten.
- **Strafrechtelijke gegevens**: strafbare feiten, verdenkingen en veiligheidsmaatregelen in het kader van bijvoorbeeld computervredebreuk.

Bewaken en beveiligen: bewaken van militaire objecten en Defensiepersoneel (artikelen 4.9 en 4.11)
Persoonsgegevens worden verwerkt in het kader van activiteiten voor de bewaken en beveiliging van militaire objecten en defensiepersoneel, wat inhoudt:

- **Gewone persoonsgegevens:** locatiegegevens en identificatie-informatie van personen binnen of rond militaire objecten en terreinen, functie en operationele rollen, camerabeelden, kentekens.
- **Gevoelige persoonsgegevens:** bewegings- en gedragsgegevens die worden verzameld via bewakingstechnologieën,[28] digitale identificatiegegevens (bijv. i.v.m. het monitoren van het Electromagnetisch Spectrum (EMS) in het kader van het beveiligen van militaire objecten).
- **Strafrechtelijke gegevens:** gegevens met betrekking tot personen die als een veiligheidsrisico worden beschouwd of betrokken zijn bij strafbare feiten.

Persoonsgegevens van (aspirant) militairen en (aankomend) Defensiepersoneel (artikelen 7.2 en 7.3 - PM)

- **Gewone persoonsgegevens**: gegevens om de persoon te identificeren (naam, adres, e-mail, registratienummer e.d.).
- **Bijzondere persoonsgegevens**: gezondheidsgegevens en biometrische gegevens in het kader van keuren en de monitoring van de gezondheid. In sommige gevallen worden er gewone en mogelijk bijzondere persoonsgegevens verwerkt van Nederlanders van 17 tot en met 27 jaar die een enquête invullen om hun belangstelling voor vrijwillige indiensttreding bij Defensie te laten weten.

[28] Camerabeelden van personen worden niet standaard als bijzondere persoonsgegevens beschouwd tenzij de verwerking specifiek gericht is op identificatie op basis van bijzondere persoonsgegevens. Zie: Beleidsregels cameratoezicht, Autoriteit Persoonsgegevens, 9 februari 2016, pagina 25-26.

3. Gegevensverwerkingen

Op basis van het wetsvoorstel en de MvT kunnen diverse verwerkingen van persoonsgegevens worden verwacht, uitgevoerd door verschillende entiteiten binnen het Ministerie van Defensie, zoals de operationele commando's en ondersteunende (IT)-diensten. Met bondgenoten en nationale veiligheidsdiensten kan ook samenwerking plaatsvinden, waarbij deze samenwerkingen gepaard gaan met gegevensverwerkingen of de samenwerking zelf als verwerking te kwalificeren is.

Hieronder worden de verwerkingen niet in een specifieke volgorde weergegeven. In de praktijk is sprake van een cyclisch proces waarbij voorafgaand aan de verwerking de informatiebehoefte wordt bepaald en de verwerking "vernietigen'' op meerdere momenten in de tijd plaatsvindt in lijn met het beginsel van dataminimalisatie uit de Algemene Verordening Gegevensbescherming (AVG).[29]

Verzamelen van persoonsgegevens
Aangezien de drie categorieën gereedstellingsactiviteiten in de informatieomgeving een ander 'doel' en andere 'uitvoerders' kennen voor het verzamelen van persoonsgegevens, vindt hieronder op die punten een nadere uitsplitsing plaats.

- **Doel:** het verzamelen van persoonsgegevens is essentieel voor het opleiden, trainen en oefenen van defensiepersoneel (artikel 4.6). Ook zijn persoonsgegevens nodig om een gedetailleerd omgevingsbeeld te verkrijgen voor operationele beslissingen (artikelen 4.7 en 4.8). Bovendien kunnen persoonsgegevens worden verzameld in het onderzoek naar potentiele dreigingen in het kader van bewaken en beveiligen (artikelen 4.10 en 4.11).
    - **Geoefendheid (opleiden, trainen en oefenen)**
      Tijdens militaire oefeningen maakt Defensie bijvoorbeeld gebruik van onbemenste systemen uitgerust met camera's en sensoren om de technische mogelijkheden te beproeven en mensen op te leiden, hen te laten oefenen en getraind te laten worden met het werken met deze middelen. Naast modellering en simulatie volgens het gereedstellingsproces vinden dergelijke oefeningen voornamelijk plaats op of boven Defensie-oefenterreinen.[30] Wanneer de oefenscenario's daarom vragen, bestaat de behoefte om deze ook boven terreinen die geen Defensie-oefenterreinen, bijvoorbeeld openbare recreatiegebieden of stedelijk gebied, plaats te laten vinden. Deze activiteiten kunnen een inbreuk maken op bepaalde rechten en vrijheden van betrokkenen. Tijdens deze activiteiten worden onvermijdelijk persoonsgegevens verzameld, zoals beelden van personen op straat. In veel gevallen is verwerken van persoonsgegevens op zich niet het doel, maar doorgaans onvermijdelijk onderdeel van de informatie die in dit kader wordt

[29] Dit beginsel ziet op de verwerking van persoonsgegevens.
[30] Waar passend wordt in het gereedstellingsproces gebruik gemaakt van een gereedstellingssystematiek met verschillende gereedstellingsniveaus. Die systematiek houdt in dat het opleiden, trainen en oefenen van militairen op vier niveaus plaats vindt en afgesloten wordt met een certificering. Binnen die vier niveaus wordt bij de eerste drie niveaus in een besloten omgeving getraind en alleen bij het vierde niveau wordt gebruik gemaakt van de publieke ruimte. Op het eerste niveau wordt op lokaal niveau getraind. Op het tweede niveau wordt getraind door middel van nabootsing, zoals een cyberrange. En op het derde niveau wordt getraind door middel van een synthetisch nagebootste omgeving. Op het vierde niveau wordt in de openbare ruimte getraind, waarbij zoveel mogelijk waarborgen zijn ingebouwd om de risico's voor derden te beperken. Een eenheid sluit het gereedstellingsproces af met een certificeringsoefening, waarbij het behalen van de certificering betekent dat de eenheid inzetgereed is.

verwerkt. Deze informatie zal doorgaans terstond kunnen worden verwijderd. In bepaalde situaties zullen deze persoonsgegevens noodzakelijk zijn voor het doel van de oefening. In sommige omstandigheden kunnen daarbij ook (meta)data[31] van elektronische communicatiemiddelen in het oefengebied worden opgevangen, welke terstond daarna worden verwijderd. In de meeste gevallen zijn de sensoren louter nodig om systemen veilig te kunnen gebruiken en in een aantal gevallen is het technisch niet mogelijk de sensoren uit te schakelen. Ook bestaat de behoefte om militairen onder meer controleerbare omstandigheden op te leiden, te laten trainen en oefenen. Dat betekent dat militairen in oefensituaties bijvoorbeeld een sporthorloge (wearable device) dragen om lichaamstemperatuur, hartslag en andere elementaire lichaamsfuncties bij te houden en te zorgen dat zij duurzaam inzetbaar blijven, ook onder extreme omstandigheden.

    - **Bewaken en beveiligen (incl. beschermen van defensiepersoneel)**
      In het kader van de digitale beveiliging van Defensie wordt openbronnen-, en social media onderzoek uitgevoerd om cyberdreigingen- en kwetsbaarheden vast te stellen en te pareren voor SEWACO. Deze activiteiten vallen voor andere organisaties binnen de werkingssfeer van de Cyberveiligheidswet en de NIS-II Richtlijn en behelzen onder meer het verzamelen van *Cyber Threat Intelligence*. Met de Wodg wordt voorzien in een grondslag voor deze activiteiten. Daarnaast worden andere type sensoren ingezet, waaronder middelen die *sweeps* van het elektromagnetisch spectrum (EMS) in de omgeving kunnen maken.
    - **Informatiepositie (omgevingsbeeld)**
      In het kader van gereedheid is het noodzakelijk dat commandanten voorzien worden van de juiste informatie om zich voor te bereiden op inzet en om de veiligheid van hun mensen en middelen te kunnen garanderen. Dat betekent dat daarvoor de behoefte bestaat aan het opbouwen van een omgevingsbeeld. Daarvoor worden open bronnen geraadpleegd (om bijvoorbeeld aan- en afvoerroutes voor verplaatsingen in kaart te brengen) en wordt gekeken naar de te verwachten weersomstandigheden, potentiele opponenten, militair, paramilitair of anderszins.

- **Gegevens:** naam, adres, leeftijd, geslacht, locatiegegevens, en digitale identificaties (zoals IP- en MAC-adressen).[32]
  - **Gewone persoonsgegevens:** namen, adressen, woonplaatsen, rangen/schalen en functies van defensiepersoneel.
  - **Gevoelige persoonsgegevens:** fysieke gegevens (geslacht, leeftijd), locatiegegevens (operationele gegevens) en gedragsinformatie verzameld tijdens oefeningen.[33]

[31] Het is in het wetsvoorstel niet altijd duidelijk of er over metadata of over inhoud van communicatie wordt gesproken. Metadata kunnen echter ook (bijzondere) persoonsgegevens bevatten.

[32] Sensoren die persoonsgegevens verzamelen, kunnen nodig zijn om het systeem waarop de sensoren aanwezig zijn, veilig te gebruiken. Het kan zijn dat het technisch onmogelijk de sensoren uit te schakelen. Sensoren die persoonsgegevens verzamelen kunnen ook onderdeel zijn van het beproeven van technische mogelijkheden en opleiden/oefenen/trainen van gebruikers. Daarnaast worden sensoren ingezet, waaronder middelen die *sweeps* van het elektromagnetisch spectrum (EMS) in de omgeving kunnen maken, om het normbeeld te bepalen of om een specifieke omgeving dicht te zetten zodat fysieke inzet en zichtbaarheid wordt verkleind en daarmee de veiligheid en onderkenning wordt verhoogd.

[33] Om na te gaan wat bijdraagt aan duurzame inzetbaarheid van militairen, worden bijvoorbeeld tijdens 'opleiden, trainen en oefenen' vitale functies zoals een hartslag, ademhaling en lichaamstemperatuur bijgehouden om prestaties te optimaliseren en gezondheidsschade te voorkomen in normale, verzwaarde en extreme omstandigheden.

- **Bijzondere persoonsgegevens:** biometrische gegevens en gezondheidsinformatie indien relevant voor specifieke trainingen van militairen.[34]
- **Uitvoerders:**
    - Geoefendheid: Faculteit Militaire Wetenschappen, scholen, opleidings- en trainingscentra en operationele onderdelen/ eenheden van Defensie.
    - Bewaken en beveiligen: operationele eenheden krijgsmacht, specifieke onderdelen/eenheden van Defensie.
    - Informatiepositie: operationele onderdelen/eenheden van de krijgsmacht.

Personeel (gezondheidsmonitoring)

- **Doel:** door het monitoren van gegevens met betrekking tot gezondheid het bevorderen (het bieden van *preventieve arbeidsgeneeskunde*) van de gezondheid van militair ambtenaren in actieve dienst.
- **Gegevens:** identificatoren met betrekking tot militair ambtenaren en gezondheidsgegevens.
- **Uitvoerders:** operationele onderdelen/eenheden van de krijgsmacht ondersteund door medische dienstverlening van Defensie.

Personeel (enquête)

- **Doel:** het verkrijgen van inzicht in de interesse en mogelijke geschiktheid van Nederlanders tussen de 17 en 27 jaar voor een militaire aanstelling bij Defensie.
- **Gegevens:** basisgegevens uit de Basisregistratie Personen en mogelijk gegevens over gezondheid.
  Uitvoerders: beleidsafdelingen van Defensie.

<u>Ordenen van persoonsgegevens</u>

- **Doel:** persoonsgegevens moeten georganiseerd worden, met daarbij specifieke aandacht voor anonimiseren en pseudonimiseren (artikel 4.2). Ook worden deze gegevens geüpdatet en veilig opgeslagen voor analyse, evaluaties, en rapportage doeleinden (artikel 4.6 en 4.10).
- **Gegevens:** trainingsgegevens, operationele logboeken, en beveiligingsmonitoringrapporten, bijgewerkte contactdetails, geactualiseerde trainingsgegevens en operationele statusrapporten.
- **Uitvoerders:** operationele onderdelen/eenheden van de krijgsmacht ondersteund door eenheden van Defensie (IT, beveiliging, informatiemanagement etc.)

<u>Analyseren van persoonsgegevens</u>

- **Doel:** het benutten en combineren van persoonsgegevens om training en inzetbaarheid te verbeteren (artikel 4.6), en voor het bijwerken van operationele plannen en veiligheidsprocedures (artikel 4.11).
- **Gegevens:** naam, leeftijd, geslacht, locatiegegevens en digitale identificaties.[35]
- **Uitvoerders:** operationele onderdelen/eenheden van de krijgsmacht ondersteund door eenheden van Defensie (IT, beveiliging, informatiemanagement etc.)

Draagbare sensortechnologie en de analyse van biometrische gegevens kan gebruikt worden om de fysieke belasting op het menselijk lichaam te monitoren en te gebruiken om veilig en verantwoord op te leiden, te trainen en te oefenen.

[35] In het kader van de informatiepositie, worden gegevens omtrent personen uit publiek toegankelijke bronnen, data van bondgenoten, derden e.d. geanalyseerd door bijvoorbeeld het combineren van verschillende databronnen. Er zal geen sprake zijn van stelselmatige online monitoring (daarbij zijn de volgende elementen van belang: duur, plaats, intensiteit of frequentie en het al dan niet toepassen van een technisch hulpmiddel dat meer biedt dan alleen versterking van de zintuigen).

Verstrekken van persoonsgegevens

- **Doel:** het delen van (al dan niet geanonimiseerde of gepseudonimiseerde) persoongsgegevens met bondgenoten en andere relevante overheidsinstanties voor samenwerking en veiligheid (artikel 4.12).
- **Gegevens:** persoonsgegevens gerelateerd aan specifieke operaties of bedreigingen.
- **Uitvoerders:** operationele onderdelen/eenheden van de krijgsmacht ondersteund door eenheden van Defensie (IT, beveiliging, informatiemanagement etc.).

Vernietigen van persoonsgegevens

- **Doel:** zorgen voor de verwijdering en vernietiging van persoonsgegevens (artikel 4.3) als onderdeel van dataminimalisatie en het voorkomen van ongeautoriseerde toegang en misbruik.
- **Gegevens:** opgeslagen persoonsgegevens binnen defensienetwerken.
- **Uitvoerders:** operationele onderdelen/eenheden van de krijgsmacht ondersteund door eenheden van Defensie (IT, beveiliging, informatiemanagement etc.).

4. Technieken en methoden van de gegevensverwerkingen

Het wetsvoorstel voorziet in het gebruik van de volgende technieken en methoden voor het verwerken van persoonsgegevens. Aangezien het wetsvoorstel beoogt zo technologie-neutraal mogelijk te opereren kan in dit hoofdstuk van de DPIA geen invulling worden gegeven aan het exact omschrijven van de technieken en methoden die kunnen of zullen worden gebruikt voor de gegevensverwerkingen zonder te speculeren/interpreteren. Daarom worden de verschillende beoogde activiteiten per cluster beschreven, met daarbij de (summiere) manier van verwerken zoals in het wetsvoorstel omschreven en een verwijzing naar het wetsartikel.

De beveiliging van de platforms, dataopslag en dataverwerking wordt nader gespecificeerd bij AMvB. Dit zal geschieden conform het Defensie Beveiligingsbeleid (DBB). Het DBB zal van toepassing zijn op het gebruik van zowel de technische middelen als de dataverwerkingen.

- **Geoefendheid (opleiden, trainen en oefenen)**
  - Verwerken van informatie met bemenste en onbemenste systemen (artikel 4.6)
  - Uitvoeren van activiteiten in het elektromagnetische spectrum (artikelen 4.6 en 4.7)
  - Verwerken van informatie uit openbare online bronnen (artikel 4.6)
  - Verwerken van informatie verkregen uit commerciële bronnen, verkregen van andere overheden en buitenlandse overheidsbronnen (artikel 4.6)
  - Experimenteren met nieuwe technologieën (waaronder artificiële intelligentie) (artikel 4.6)
  - Geïntegreerd trainen en gereedstellen met sensoren d.m.v. algoritmes en andere technologieën (artikel 4.6)
- **Informatiepositie**
  Verwerken van informatie met sensoren (artikelen 4.7 en 4.8)
  - Uitvoeren van activiteiten in het elektromagnetische spectrum (artikelen 4.7, 4.8 en 4.9)
  - Verwerken van informatie uit openbare online bronnen (artikelen 4.7 en 4.8)
  - Verwerken van informatie verkregen uit commerciële bronnen, verkregen van andere overheden en buitenlandse overheidsbronnen (artikel 4.7 en 4.8)
- **Bewaken en beveiligen**
  - Het beveiligen (defensief) van de digitale infrastructuur (zoals wifipunten en draadloze netwerken (artikelen 4.9 en 4.10)
  - Verwerken van informatie uit openbare online bronnen ten behoeve van cyber threat intelligence (artikelen 4.9, 4.10 en 4.11)
  - Verwerken van informatie verkregen uit commerciële bronnen, verkregen van andere overheden en buitenlandse (artikel 4.10)
  - Overheidsbronnen (artikelen 4.10 en 4.11)
  - Mogelijk gebruik van geavanceerde en innovatieve technologieën, zoals artificiële intelligentie, ten behoeve van defensieve IT- en netwerk beveiliging (artikel 4.10)
- **Personeel**
  - in het kader van preventieve gezondheidszorg technische middelen laten dragen om de gezondheid proactief te monitoren (artikel 7.3).
  - Gegevens van Nederlanders (17-27 jaar) in het kader van de werving via een enquête **(Hoofdstuk 5, artikel 5.1).**

5. Verwerkingsdoeleinden

De Wodg heeft tot doel om middels een wet in formele zin kaders te stellen voor het tijdig gereedstellen van de krijgsmacht onder de verantwoordelijkheid van de minister van Defensie. Zowel voor de activiteiten van de krijgsmacht zelf als door ondersteunende activiteiten van andere onderdelen van het ministerie van Defensie. Het doel van de toepassing van dit kader is een daadwerkelijke en stelselmatige gereedheid van het militair vermogen, en afstemming van dit belang met andere belangen in een weerbare maatschappij.[36]

De uitwerking van deze doelstelling van de Wodg is toegelicht in het eerste hoofdstuk van de MvT. De verschillende gereedstellingsactiviteiten die plaatsvinden in de informatieomgeving kunnen, zoals hiervoor benoemd, worden onderverdeeld in drie taakgebieden. De doeleinden waarvoor de gegevensverwerkingen plaatsvinden, worden hierna per categorie geduid. Aanvullend wordt ingegaan op personele gereedheid.

1. **Geoefendheid (opleiden, trainen en oefenen)**
Doel: het voorbereiden en onderhouden van de geoefendheid van de krijgsmacht om hun gereedheid en capaciteit voor operationele inzet te waarborgen. Persoonsgegevens worden verwerkt voor het produceren van kennis, het ontwerpen en ontwikkelen van opleidingen en trainingen, het volgen van opleidingen en het trainen en oefenen met bepaalde activiteiten om tot gereedheid/een bepaalde geoefendheid te komen.

2. Informatiepositie (omgevingsbeeld)
Doel: Commandanten voorzien van de juiste informatie om zich voor te bereiden op inzet en om de veiligheid van hun mensen en middelen te kunnen garanderen. Dat betekent dat daarvoor de behoefte bestaat aan het opbouwen van een norm- en omgevingsbeeld in de fase voorafgaand aan inzet van de krijgsmacht, maar voordat de regering een besluit tot inzet heeft genomen. Daarbij staat informatie over actoren en factoren in de focusgebieden en dreigingen van buitenaf centraal (*situational awareness / situational understanding)*.

3. Bewaken en beveiligen (incl. beschermen van defensiepersoneel)
Doel: het waarborgen van de veiligheid van defensieactiviteiten, locaties, faciliteiten en informatie. Dit omvat zowel fysieke beveiliging van Defensielocaties als de bescherming van digitale infrastructuren tegen potentiële bedreigingen. Dit is een randvoorwaarde voor het kunnen bereiken en behouden van een toestand van gereedheid.

4. Persoonsgegevens van (te werven) militairen
Doel: het waarborgen van de gezondheid van militairen in werkelijke dienst waaronder het sneller kunnen beoordelen van de geschiktheid (keuren), epidemiologisch onderzoek en het monitoren van de gezondheid van de militair om eerder en beter risico's te kunnen signaleren. Het werven van Nederlanders vanaf 17 jaar door het toesturen van een enquête heeft tot doel om inzicht te krijgen in de interesse en mogelijke geschiktheid van Nederlanders tussen 17-27 jaar voor een aanstelling als militair ambtenaar bij Defensie. De enquête is een instrument dat het dienmodel en daarmee de schaalbare krijgsmacht als geheel ondersteunt en een noodzakelijk onderdeel van de personele gereedheid vormt.

[36] MvT, voorlopig ontwerp Wodg, versie 2.1.

6. Betrokken partijen

De gegevensverwerkingen worden uitgevoerd door Defensie en kunnen samenwerking met zowel nationale als bondgenootschappelijke entiteiten omvatten. Hierbij vindt gegevensverstrekking plaats indien noodzakelijk voor internationale samenwerking en operationele vereisten.

Defensieambtenaren en niet-werknemers die in de uitoefening van hun functie onder het gezag van de Minister van Defensie persoonsgegevens verwerken zijn in de zin van het wetsvoorstel niet aan te merken als 'ontvanger' of 'betrokkene'.

Betrokken partijen en hun rol:

- **Minister van Defensie**
  - **Rol:** Verwerkingsverantwoordelijke in de zin van de AVG[37]
  - **Toelichting:** de Minister draagt zorg voor de gereedstelling van de krijgsmacht en is verantwoordelijk voor het verwerken van persoonsgegevens op grond van de Wodg.

- **Defensieambtenaren (commandanten[38], beroepsmilitairen, reservisten en burgerpersoneel)**[39]
  - **Rol:** betrokkenen
  - **Toelichting:** deze groep omvat militairen aangesteld bij de krijgsmacht en burgers aangesteld bij Defensie wier persoonsgegevens worden verwerkt voor operationele en administratieve/bedrijfsvoering doeleinden.

- **Medewerkers en personeelsleden van (bondgenootschappelijke) krijgsmachten**[40] **(NAVO-bondgenoten en EU-partners)**
  - **Rol:** betrokkenen, derde, ontvanger, (gezamenlijke) verwerkingsverantwoordelijke
  - **Toelichting:** er kan sprake zijn van gezamenlijke gegevensverwerking en uitwisseling van persoonsgegevens kunnen plaatsvinden in het kader van bondgenootschappelijke/EU samenwerking.

- **Niet-werknemers Defensie. Personen met een andersoortige (arbeids-)relatie met Defensie dan een aanstelling zoals inhuur, uitzendkrachten, bezoekers, enz.**
  - **Rol:** betrokkenen
  - **Toelichting:** informatie over deze betrokkenen kan worden verwerkt voor operationele en administratieve/bedrijfsvoering doeleinden.

---

[37] De Minister van Defensie is verwerkingsverantwoordelijke in de zin van AVG, zie Regeling AVG Defensie, artikel 1.2 lid 1.

[38] Militair, verantwoordelijk voor het voorbereiden, leiden en beëindigen van operaties. Zie *NATO Command: The authority vested in a member of the armed forces for the direction, coordination, and control of military forces.*

[39] Het gaat hierbij om burgers en militairen die aangesteld zijn bij de krijgsmacht en Defensie. Zie Wet ambtenaren defensie artikel 1a: 1. militaire ambtenaren: zij, die zijn aangesteld bij het beroepspersoneel van de krijgsmacht of bij het reservepersoneel van de krijgsmacht om in militaire openbare dienst werkzaam te zijn, 2. burgerlijke ambtenaren: burgerlijke ambtenaren die zijn aangesteld om werkzaam te zijn bij het Ministerie van Defensie.

[40] Het gaat hierbij om doelgroepen die functionele relatie hebben met Defensie. Hierbij valt te denken aan rijksambtenaren, medewerkers van NAVO en EU-bondgenoten en strategische partners, maar ook medewerkers van veiligheidsregio's en civiele partners. Het kan ook gaan om betrokkenen van potentiële militaire tegenstanders (strijdkrachten en andere groeperingen).

- **Individuele personen en groepen van personen die bedoeld onderdeel zijn van een verwerking van persoonsgegevens**[41]
    - **Rol:** betrokkenen
    - **Toelichting:** informatie over deze betrokkenen kan worden verwerkt om operationele veiligheid en besluitvorming te ondersteunen, gegeven een opdracht.

- **Burgers (civiele personen/partijen)**[42]
    - **Rol:** betrokkenen
    - **Toelichting:** dit omvat personen of groepen in Nederland en wereldwijd, die onderdeel kunnen zijn van een verwerking van persoonsgegevens gegeven een opdracht, bijvoorbeeld bij maatschappelijk relevante ontwikkelingen in de operationele omgeving. Het gaat hierbij om betrokkenen die geen functionele relatie hebben met Defensie.
        - **Onbedoeld/ongericht**: Personen/groepen (incl. burgers) die mogelijk een risico lopen dat diens persoonsgegevens worden verwerkt, omdat zij bijvoorbeeld in de omgeving van een Defensielocatie of oefengebied wonen. Hoewel de verwerking van deze persoonsgegevens op zich niet het doel is, kan het onvermijdelijk onderdeel zijn van de informatie die wordt verwerkt.

- **Overheidsinstanties, internationale organisaties (bv. NAVO) en EU**
    - **Rol**: verstrekker of ontvanger van persoonsgegevens
    - **Toelichting**: andere overheidsorganisaties, internationale organisaties (bv. NAVO, Internationale Rode Kruis) of EU instituties (*European Defence Agency*) vervullen een rol in de gereedstellingssystematiek waarbij de uitwisseling van persoonsgegevens noodzakelijk is.[43]

- **Externe IT-dienstverleners**
    - **Rol:** verwerker/sub-verwerker
    - **Toelichting:** deze partijen ondersteunen de technische aspecten van gegevensverwerking en kunnen als verwerker worden aangemerkt bij het verwerken van persoonsgegevens namens Defensie.

- **Nederlanders van 17-27 jaar die een enquête ontvangen**
    - **Rol:** verstrekker van persoonsgegevens
    - **Toelichting:** deze Nederlanders verstrekken informatie via een enquête over hun interesse en mogelijke geschiktheid voor een aanstelling als militair ambtenaar.

---

[41] Bv.: (potentiele) opponenten, militair, paramilitair of anderszins, maar bijvoorbeeld ook publieke figuren, journalisten, opiniemakers.

[42] Het gaat hierbij om betrokkenen die geen functionele relatie hebben met Defensie. Denk hierbij aan (civiele) burgers wereldwijd waaronder publieke figuren en journalisten die bedoeld of onbedoeld onderdeel zijn van een verwerking van persoonsgegevens.

[43] Om gereed te zijn dienen gereedstellingsactiviteiten verricht te worden. Dit ziet op activiteiten ten behoeve van de personele en materiële gereedheid en de geoefendheid. Deze activiteiten vinden plaats in de fysieke leefomgeving, maar ook online, waarbij bedoeld en onbedoeld persoonsgegevens verwerkt worden. Als onderdeel van de gereedheid van de krijgsmacht is ook vereist dat zij beschikt over informatie over actoren en factoren in potentiële inzetgebieden en dreigingen van buitenaf. Die informatiepositie heeft als doel om te zorgen dat de krijgsmacht veilig ingezet wordt (personele veiligheid) en proportioneel en doeltreffend handelt. Het is in de operationele omgeving van essentieel belang om een onderscheid te maken tussen gewone burgers en militairen of andere gevaarlijke actoren en tussen civiele infrastructuur en militaire doelwitten.

7. Belangen bij de gegevensverwerkingen

De Wodg streeft naar een evenwicht tussen het vitale belang van daadwerkelijke en stelselmatige gereedheid en individuele belangen, rechten en vrijheden van individuen, in lijn met (inter)nationale wetgeving en verdragen.

1. **Geoefendheid (opleiden, trainen en oefenen)**
   - **Doel**: het voorbereiden en onderhouden van de geoefendheid van militaire eenheden om hun gereedheid voor operationele inzet te waarborgen. Persoonsgegevens worden verwerkt voor het produceren van kennis, het ontwerpen en ontwikkelen van opleidingen en trainingen, het volgen van opleidingen en het trainen en oefenen met bepaalde activiteiten om tot gereedheid/een bepaalde geoefendheid te komen.
   - **Belang**:
     - **Minister van Defensie**: de Minister is verantwoordelijk voor de gereedheid van Defensie en is voor de verwerking van persoonsgegevens in het kader van de gereedheid verwerkingsverantwoordelijke in de zin van de AVG.
     - **Defensiepersoneel**: heeft belang bij nauwkeurige en veilige verwerking van hun persoonsgegevens die relevant zijn om hun opleiding, training, inzetbaarheid en hun persoonlijke veiligheid en ontwikkeling te ondersteunen.
     - **NAVO-bondgenoten/EU**: hebben belang bij gezamenlijke trainingsinspanningen die de interoperabiliteit en gezamenlijke inzetbaarheid vergroten, voor zover daarvoor de verwerking van persoonsgegevens noodzakelijk is. Deze verwerking draagt bij aan de collectieve veiligheid.
     - **Burgers**: hebben belang bij (1) de versterking van de nationale en bondgenootschappelijke veiligheid en (2) de bescherming van hun privacyrechten.

2. **Informatiepositie (omgevingsbeeld)**
   - **Doel**: het vergaren en analyseren van persoonsgegevens om een beeld van de operationele omgeving te vormen voor een veilig en doeltreffend optreden van eenheden of onderdelen van de krijgsmacht (*situational awareness/understanding*).
   - **Belang**:
     - **Minister van Defensie**: heeft belang bij het verzamelen en analyseren van persoonsgegevens om de capaciteiten te versterken en bedreigingen tijdig te identificeren, in overeenstemming met internationale verdragen.
     - **Defensiepersoneel**: hebben belang bij het kunnen verwerken van de relevante persoonsgegevens die noodzakelijk zijn om de taken/functie effectief te kunnen uitoefenen en ondersteunen.
     - **NAVO-bondgenoten/EU**: hebben belang bij samenwerking en het delen van persoonsgegevens om de collectieve defensiecapaciteit te verbeteren en bij te dragen aan de collectieve veiligheid.
     - **Externe IT-dienstverleners**: hebben een commercieel belang bij het leveren van diensten die gegevensverwerking en de beveiliging van informatiesystemen ondersteunen.
     - **Burgers**: hebben belang bij (1) de versterking van de nationale en bondgenootschappelijke veiligheid en (2) de bescherming van hun privacyrechten.

3. **Bewaken en beveiligen (incl. beschermen van defensiepersoneel)**
    - **Doel**: het waarborgen van de veiligheid van defensieactiviteiten, locaties, faciliteiten en informatie.
    - **Belang**:
        - **Minister van Defensie**: heeft belang bij de bescherming en beveiliging van militairen objecten, en digitale infrastructuur en data van Defensie en het voorkomen van inbreuken op de veiligheid van operaties, conform internationale verplichtingen zoals vastgelegd in het Noord-Atlantisch Verdrag.
        - **Defensiepersoneel**: heeft belang bij veilige werkomstandigheden, getraindheid en geoefendheid, bij de waarborging van persoonlijke veiligheid binnen hun operationele en bedrijfsmatige omgeving en bij het kunnen verwerken van de relevante persoonsgegevens die noodzakelijk zijn om de taken/functie in het kader van bewaken en beveiligen effectief te kunnen uitoefenen.
        - **Burgers**: hebben belang bij (1) de handhaving van nationale en bondgenootschappelijke veiligheid en (2) de bescherming van hun privacyrechten.

4. **Persoonsgegevens die worden verwerkt in het kader van de gezondheid van militairen en werving**
    - **Doel:** het bewaken (monitoren) en bevorderen van de gezondheid van militairen in werkelijke dienst, het verrichten van epidemiologisch onderzoek, en het werven van Nederlanders door het toesturen van een enquête.
    - **Belang:**
        - **Minister van Defensie:** heeft belang bij het inzetbaar houden van militairen en hun gezondheid zo lang mogelijk in een optimale conditie houden. Daarnaast heeft de Minister belang dat de krijgsmacht voldoende personele capaciteit heeft die schaalbaar kan meebewegen met de dreiging. Een toekomstbestendige krijgsmacht die in staat is snel op te schalen in de aanloop naar een conflictsituatie.
        - **Defensiepersoneel:** heeft een belang bij het zo veilig en effectief mogelijk hun werkzaamheden uitvoeren.
        - **Nederlanders van 17-27 jaar:** een beter beeld te verkrijgen over de mate van interesse en mogelijke geschiktheid voor een aanstelling als militair bij Defensie.

8. Verwerkingslocaties

Defensie IT-infrastructuur: geen transfer/doorgiftemechanisme van toepassing
Voor zover de verwerking van persoonsgegevens plaatsvindt op Defensielocaties en IT-infrastructuur van Defensie binnen- en buiten het Koninkrijk geldt dat de digitale verwerkingslocatie Nederland is. Dat het platform waarmee persoonsgegevens worden verzameld op dat moment buiten Nederland is 'gesitueerd', betekent niet dat er sprake is van een doorgifte in de zin van de AVG. Wanneer er sprake is van een uitwisseling over de IT-systemen van Defensie, is er naar de opinie van de European Data Protection Board (EDPB) geen sprake van een doorgifte en is er geen doorgiftemechanisme noodzakelijk.[44]

Doorgiftemechanisme civiele organisaties
Opslaan van persoonsgegevens maakt onderdeel uit van het begrip verwerking. Als gebruik wordt gemaakt van externe cloudaanbieders buiten de Europese Economische Ruimte (EER)kan er gebruik gemaakt worden van bestaande waarborgen zoals adequaatheidsbesluiten en standaardcontractbepalingen, voorzien in de AVG.

Doorgiftemechanisme bondgenoten
De Wodg voorziet in (gepseudonimiseerde) doorgiften aan bondgenoten in verband met het doeltreffend optreden in de operationele omgeving in bondgenootschappelijk verband; of in verband met het beveiligen van de netwerk- en informatiesystemen van deze bondgenoot.[45] In de meeste situaties voorzien in de Wodg kan geen gebruik gemaakt worden van een adequaatheidsbesluit van de Europese Commissie, doordat deze voor bijvoorbeeld de Verenigde Staten, Canada en NAVO als internationale organisatie ontbreekt. De ontvangende organisaties zullen vanwege soevereiniteitsoverwegingen geen gebruik kunnen, willen of mogen maken van *standard contractual clauses.* Ook andere doorgiftemechanismes zijn niet van toepassing of mogelijk in deze doorgiftesituaties.

Voor specifieke situaties, waarin bij wet is voorzien, kent de AVG een uitzonderingsbepaling zoals gedefinieerd in artikel 49, lid 1, sub d. Deze uitzonderingsbepaling kan, door de wijze waarop de Wodg daar in artikel 4.12 lid 1 sub f, voorziet, worden gebruikt.

De EDPB geeft aan dat, hoewel het gebruik van artikel 49 in tijd en frequentie niet beperkt wordt krachtens overweging 112 van de AVG, dit geen structurele oplossing zou moeten bieden voor de doorgifte van persoonsgegevens. Grootschalige en systematische doorgiften dienen idealiter nog steeds gebaseerd te worden op passende waarborgen bij de ontvanger, zoals bedoeld in artikel 46 AVG. Wanneer doorgiften plaatsvinden op basis van de bij wet voorziene uitzonderingsmogelijkheid, geldt dat per doorgifte een analyse ten aanzien van de noodzakelijkheid van die verstrekking dient te worden uitgevoerd.[46]

Het gebruik van een uitzonderingsgrond brengt risico's voor het beschermingsniveau van de verstrekte persoonsgegevens met zich mee. Waar de uitzonderingsgrond ex artikel 49 AVG wordt gebruikt, bieden ontvangers van persoonsgegevens onvoldoende bescherming bij het verwerken van die

[44] EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR – voorbeeld 5, p6/7
[45] Artikel 4.10, sub f Wodg.
[46] European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 mei 2018, p. 10-11; MvT, Voorlopig ontwerp Wodg p. 112

persoonsgegevens of kan het beschermingsniveau niet voldoende worden beoordeeld. Deze verstrekkingsgrond kan enkel worden gebruikt indien de Minister van Defensie betrokken is bij internationale (beleids-)afspraken (bijv. in de vorm van een samenwerkingsafspraak in een Memorandum of Understanding of anderszins). Ook kunnen er afspraken ten aanzien van de (wijze van) verwerking van persoonsgegevens worden gemaakt in dergelijke internationale afspraken.

9. Juridisch en beleidsmatig kader

Gezien de aard van deze DPIA is een limitatieve opsomming van wet- en regelgeving niet mogelijk. Gevoegd de meest relevante algemene kaders en de specifieke voor informatieomgeving en personeel.

Specifiek voor de AVG dient te worden opgemerkt dat de AVG als gegevensbeschermingskader voor de verwerking van persoonsgegevens in het kader van hoofdstukken 1 tot en met 4 van het wetsvoorstel van overeenkomstige toepassing is, met uitzondering van de artikelen 9, 10, hoofdstuk III (rechten van de betrokkenen) en de artikelen 33, 34 en 36 van de AVG en de artikelen 22 tot en met 33 van de UAVG. Zie ook paragraaf 4.5 van de MvT Wodg.

Voor de overige hoofdstukken van dit wetsvoorstel geldt de AVG en UAVG onverkort. Deze zullen aldus gelden voor de gegevensverwerkingen die op grond van de wet uiteindelijk zullen plaatsvinden in het kader van personeel (en inkoop).

Verdragen		
Noord-Atlantisch Verdrag (NAVO-verdrag)		Algemeen
Europees Verdrag voor de Rechten van de Mens (EVRM)		Algemeen
C108+ (Conventie 108+ voor gegevensbescherming)		Algemeen
AVG & UAVG	Voor hoofdstukken 1 t/m 4 van het wetsvoorstel zijn uitgezonderd: de artikelen 9, 10, hoofdstuk III en de artikelen 33, 34 en 36 van de AVG en de artikelen 22 tot en met 33 van de UAVG.	Algemeen
AI Verordening		Algemeen
Statuut voor het Koninkrijk der Nederlanden	Artikelen 3(1) en 42(3) beschrijven de verantwoordelijkheid en bevoegdheden van het Koninkrijk met betrekking tot defensie.	Algemeen
Wetten		
Grondwet	Artikel 10 (privacy), artikel 44 (instellen ministerie, leiding minister), artikel 97 (krijgsmacht, oppergezag), artikel 98 (samenstelling krijgsmacht, militaire dienst) (artikel 100 artikel 110 (openbaarheid van bestuur)	Algemeen
Wet op de inlichtingen- en veiligheidsdiensten 2017		Informatie-omgeving
Politiewet	Artikel 4 PW KMar en Bijstand (hoofdtaak 3)	Informatie-omgeving
Wet Politiegegevens	Artikel 8 (uitvoering dagelijkse politietaak), artikel 9 (onderzoek in verband met de handhaving van de rechtsorde in een bepaald	Informatie-omgeving

	geval), artikel 10 (inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde)	
Wet Justitiële en strafvorderlijke gegevens		Informatie-omgeving
Arbeidsomstandigheden Wet		Personeel
Ambtenarenwet	Artikel 9 (geheimhouding)	Personeel
Wet ambtenaren Defensie	Artikel 12a lid 3 (geheimhouding), artikel 12bis (gedragen als goed werkgever en goed werknemer), artikel 12ter (gedragscode), artikel 12 quarter (eed/belofte)	Personeel
Algemene wet bestuursrecht		Algemeen
Archiefwet 1995	Archiefbescheiden, duurzaam toegankelijke overheidsinformatie, bewaar- en vernietigingsplicht, selectielijst	Algemeen
Telecommunicatiewet		Informatie-omgeving
Wet bescherming staatsgeheimen	Verboden plaats ter bescherming gegevens, belang veiligheid staat / in het belang van de landsverdediging	Algemeen
Wet beveiliging netwerk- en informatiesystemen (WBNI)		Informatie-omgeving
Wet open overheid	Actieve en passieve openbaarmaking	Algemeen
Cyberbeveiligingswet[47]		Informatie-omgeving
Wet weerbaarheid kritieke entiteiten[48]		Informatie-omgeving
Wet basisregistratie personen		Personeel
Rijkswet geweldgebruik defensiepersoneel	Artikel 2 (Geweldsbevoegdheid aangewezen objecten)	Informatie-omgeving
Kaderwet dienstplicht	Artikel 5 (bericht van inschrijving)	Personeel
Wet op de medische keuringen		Personeel
Regelingen		
Coördinatiebesluit organisatie, bedrijfsvoering en informatiesystemen rijksdienst		Informatie-omgeving, Algemeen
Regeling gedragsregels gebruik e-mail en		Algemeen

[47] Deze wet is nog niet van kracht.
[48] Deze wet is nog niet van kracht.

internetvoorzieningen Defensie		
Regeling AVG Defensie		Algemeen
Regeling Wpg Defensie		Informatie-omgeving
Regeling Gegevensbescherming Militaire Operaties[49]		Algemeen
Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR)		Algemeen
Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2013 (VIRBI)		Algemeen
Beleid/Overig		
Defensienota 2024		Algemeen
Nieuwe strategie voor de Europese defensie industrie		Algemeen
Permanente Gestructureerde Samenwerking		Algemeen
Gemeenschappelijk Veiligheids- en Defensiebeleid		Algemeen
Aanwijzing Gereedstelling Defensie (AGDEF)		Algemeen
Privacy Governance & Beleid (in concept)		Algemeen
Aanwijzing SG-003 Defensiebeveiligingsbeleid en onderliggende stukken		Algemeen
Aanwijzing-DGB-CIO-100 Data Governance		Algemeen
Aanwijzing DGB-CIO-101 Aanwijzing Algoritmes (concept)		Algemeen
Aanwijzing SG-989 Interne voorvalonderzoeken Defensie		Personeel
EDPB Recommendations European Essential Guarantees for surveillance measures		Informatie-omgeving
Algemene juridische kaders voor activiteiten van de krijgsmacht in de informatieomgeving, DJZ, april 2021		Informatie-omgeving
Besluit beveiliging gegevens telecommunicatie		Informatie-omgeving
Ontwerpbesluit houdende vaststelling van regels over afwijkend gebruik van frequentieruimte		Informatie-omgeving
Baseline Informatiebeveiliging Overheid (BIO)		Algemeen

[49] De regels die van toepassing zijn bij de inzet van de krijgsmacht zijn opgenomen in de Regeling Gegevensbescherming Militaire Operaties. Met dit wetsvoorstel wordt beoogd deze regels in een algemene maatregel van bestuur op te nemen.

Defensie Strategie Data Science en AI 2023-2027		Algemeen
Beleidsuitgangspunten, kabinetsreactie op rapport "Big Data in een vrije en veilige samenleving" van de WRR		Algemeen
AIV Adviesrapport Hybride dreigingen en maatschappelijke weerbaarheid		Informatie-omgeving
WRR rapport Nederland in een fragmenterende wereldorde		Algemeen
HCSS, Hybride Dreigingen en Hybride Oorlog: Consequenties voor de Koninklijke Landmacht		Informatie-omgeving
Ducheine, P.A.L. en Pijpers, Peter en Zwanenburg, Marten, Tanden voor de Leeuw, Een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving. (4 april 2024). Faculteit Militaire Wetenschappen, NLDA.		Informatie-omgeving
Cie Brouwer Grondslag gezocht. *Kamerstukken II*, 2022/23, 32761, nr. 258		Informatie-omgeving

10. Bewaartermijnen

Het wetsvoorstel bepaalt in artikel 4.2 lid 1 onder algemene waarborgen dat persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt worden verwijderd. Daarnaast is bepaald dat persoonsgegevens die niet zijn verwijderd geanonimiseerd dan wel gepseudonimiseerd worden, rekening houdend met een aantal voorwaarden, tenzij het doel zich hiertegen verzet (artikel 4.2 lid 2).

Persoonsgegevens of gepseudonimiseerde gegevens worden niet langer dan twee jaar bewaard (artikel 4.3 lid 1), tenzij de Minister het noodzakelijk acht om de bewaartermijn telkens voor ten hoogste een jaar te verlengen (artikel 4.3 lid 2). Dit betekent dat de bewaartermijn oneindig kan zijn. Per geval zal moeten worden beoordeeld of een verlenging van de bewaartermijn voor een specifieke set van persoonsgegevens aan de AVG-beginselen (artikel 5 AVG) en proportionaliteiteisen voldoet. Het is tevens mogelijk dat er via AMvB nadere regels worden gesteld over het beperken van de bewaartermijn voor specifieke verwerkingen en het opstellen van een procedure voor de verlenging van de bewaartermijn (artikel 4.3 lid 3 onder a en b).

Het wetsvoorstel zorgt enerzijds ervoor dat persoonsgegevens verwijderd worden en anderzijds gepseudonimiseerd worden bewaard.

B Beoordeling rechtmatigheid gegevensverwerkingen

11. Rechtsgrond

Het wetsvoorstel Wodg biedt de rechtsgrond voor de verwerkingen van persoonsgegevens in het kader van activiteiten die Defensie als onderdeel van haar publieke taken, zoals genoemd in het wetsvoorstel, uitvoert. Deze rechtsgrond kan worden gebruikt in combinatie met artikel 6, lid 1, sub e AVG (taak van algemeen belang).

12. Bijzondere persoonsgegevens

In het kader van de Wodg kan het verwerken van bijzondere of strafrechtelijke persoonsgegevens onvermijdelijk zijn voor de uitvoering van specifieke defensietaken, zoals medische keuringen, veiligheids- en beveiligingsmaatregelen, en inzetbaarheid. Persoonsgegevens van strafrechtelijke aard kunnen onvermijdelijk zijn bij het bewaken en beveiligen van militaire objecten en personeel.

De Wodg introduceert specifieke uitzonderingsgronden die deze verwerkingen mogelijk maken.De uitzonderingsgronden die specifiek zijn gecreëerd worden gerechtvaardigd geacht binnen het kader van de daadwerkelijke en stelselmatige gereedheid van het militair vermogen.

Artikel 4.5 van het wetsvoorstel biedt drie aanvullende waarborgen ten aanzien van de verwerking van bijzondere persoonsgegevens. De verwerking moet onvermijdelijk zijn, vindt alleen plaats in aanvulling op andere gegevens en moeten afdoende beveiligd zijn.[50]

Bijzondere persoonsgegevens:

- **Artikel 4.5 van de Wodg** creëert onder andere de mogelijkheid om gezondheids- en biometrische gegevens te verwerken voor de beoordeling en monitoring van de gezondheid van militairen, noodzakelijk voor de bescherming van vitale belangen van defensiepersoneel. Deze bepaling van het wetsvoorstel is in lijn met de vereisten die artikel 6 van Conventie 108+ van de Raad van Europa aan de verwerking van deze persoonsgegevens stelt.
- De verwerking van persoonsgegevens in het kader van bewaken en beveiligen, zoals beschreven in **artikelen 4.9-4.11**,is toegestaan, in lijn met voornoemd artikel van Conventie 108+.

Strafrechtelijke persoonsgegevens:

- De Wodg voorziet in de verwerking van strafrechtelijke gegevens onder toezicht van de overheid, zoals vastgelegd in **artikel 4.11 van de Wodg**.

[50] Het wetsvoorstel heeft daarmee voldaan aan de vereisten inzake de verwerking van bijzondere categorieën van persoonsgegevens ex. artikel 6 *Conventie voor de bescherming van personen met betrekking tot de automatische verwerking van persoonsgegevens (Conventie 108+)*, Raad van Europa.

13. Doelbinding

De verwerking van persoonsgegevens moet aan een specifiek, gerechtvaardigd en noodzakelijk doel verbonden zijn. Doeleinden dienen ook expliciet te zijn. In het kader van de Wodg zijn de beoogde verwerkingen van persoonsgegevens afgestemd op de doelen van gereedheid, zoals gedefinieerd in artikel 1.2 van de Wodg en verder toegelicht in de MvT.

Doelen van gereedheid
De daadwerkelijke en stelselmatige gereedheid van het militaire vermogen wordt beschouwd als een ondeelbaar en vitaal publiek belang. Het bereiken van gereedheid krijgt in ieder geval gestalte door de gereedstelllingsactiviteiten zoals eerder omschreven, en hieronder samengevat:

- **Geoefendheid en Gereedheid:** werven, selecteren, opleiden en trainen van personeel (incl. testen en oefenen met materieel) (artikel 2.1 lid 2a-c).
- **Informatiepositie:** Opbouwen en onderhouden van een informatiepositie (artikel 2.1 lid 2d).
- **Bewaken en Beveiligen:** Veiligheid van militaire middelen en personeel (artikel 2.1 lid 2e).

Deze elementen zijn integraal onderdeel van de gereedstellingsactiviteiten.

Samenwerking
Stelselmatige gereedheid vereist samenwerking met burgerlijk gezag en andere partners binnen een weerbare maatschappij, in lijn met de "*whole of society*" benadering van de NAVO. Gelet op de doelstellingen van de Wodg, geeft de Minister van Defensie gestalte aan deze publieke taak door zowel permanente als tijdelijke activiteiten of voorzieningen te ontplooien die nodig zijn voor het waarborgen van gereedheid.

Waarborgen van doelbinding en verdere verwerking
Doelbinding fungeert als een waarborg voor privacy en gegevensbescherming en voorkomt dat persoonsgegevens onder verantwoordelijkheid van de Minister van Defensie verder worden verwerkt zonder toetsing van hun verenigbaarheid met de oorspronkelijk vastgelegde doeleinden in het wetsvoorstel.

Het wetsvoorstel bepaalt onder de algemene waarborgen dat persoonsgegevens niet voor een ander doel verwerkt worden dan waarvoor zij zijn verkregen, tenzij deze wet, het Unierecht of een volkenrechtelijke verplichting uitdrukkelijk daarin voorziet of de Minister van Defensie hiervoor toestemming verleent, en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel (artikel 4.2 lid 4). Hiermee is de vereiste doelbinding en noodzakelijkheid conform de AVG opgenomen en wordt voorkomen dat gegevens die rechtmatig zijn verworven voor een bepaald doel ook gebruikt kunnen worden voor een ander doeleinde.

Bij elke verwerking van persoonsgegevens moet expliciet worden bepaald waarvoor deze plaatsvindt. Verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor zij aanvankelijk werden verzameld, moet zorgvuldig worden beoordeeld op verwantschap met het oorspronkelijke doeleinde, conform de kaders van de AVG. Verdere verwerking is volgens het wetsvoorstel slechts mogelijk in de specifieke gevallen (artikel 4.12), op grond van artikel 6, vierde lid, van de AVG of als dit uit een volkenrechtelijke verplichting volgt. In alle gevallen dient de verdere verwerking noodzakelijk te zijn voor dat andere doel en dient die verwerking proportioneel te zijn.

Artikel 4.2 lid 3 regelt een specifieke situatie van (verdere) verwerking in het geval dat niet bekend is of een set aan gegevens persoonsgegevens bevat die noodzakelijk zijn voor het verwerkingsdoel en daardoor niet verenigbaar zijn met de doelbinding van de verwerking. Dit kan gaan om gegevens die gecodeerd of in een vreemde taal zijn opgenomen. Op dat moment is nog niet bekend of deze gegevens persoonsgegevens bevatten, waarbij een verdere verwerking van persoonsgegevens kan plaats vinden om dit te verduidelijken. Volgens de artikelsgewijze toelichting in de MvT moet de verdere verwerking, om erachter te komen of de gegevens persoonsgegevens bevatten, zo snel mogelijk plaatsvinden na de verwerving om te voorkomen dat onnodig lang persoonsgegevens bewaard blijven. In het geval dat duidelijk is geworden dat het om persoonsgegevens gaat, dienen deze verwerkt te worden overeenkomstig het wetsvoorstel, waaronder het mogelijk verwijderen van deze persoonsgegevens.

Gegevensverstrekking
Artikel 4.12 voorziet in een gesloten verstrekkingsregime van persoonsgegevens die op grond van het wetsvoorstel worden verwerkt. Dit houdt in dat verstrekking van gegevens door de defensieonderdelen alleen mogelijk is, indien het wetsvoorstel daarin voorziet. Een gesloten verstrekkingsregime is wenselijk vanwege het bijzondere karakter van de gegevens die door de krijgsmacht worden verwerkt. Aan de ontvanger kunnen alleen persoonsgegevens worden verstrekt onder de voorwaarde dat die gegevens slechts verwerkt worden voor het doel van de verstrekking. Dat betekent dat persoonsgegevens niet mogen worden verstrekt als onvoldoende is gewaarborgd dat de gegevens niet zullen worden gebruikt voor een ander doel dan waarvoor deze zijn verstrekt. De Minister van Defensie kan op verzoek van de ontvanger onder vermelding van buitengewone omstandigheden toestemming verlenen voor de verwerking voor een ander doel.

14. Noodzaak en evenredigheid

Het wetsvoorstel voorziet in verschillende bevoegdheden voor Defensie waarvoor het verwerken van persoonsgegevens noodzakelijk is en waarbij een inbreuk op de persoonlijke levenssfeer te voorzien is. Deze paragraaf beoordeelt of de inbreuken op de persoonlijke levenssfeer en de gegevensverwerkingen noodzakelijk en evenredig zijn voor het verwezenlijken van de verwerkingsdoeleinden. Daarvoor is het van belang om te overwegen of de verwerking van persoonsgegevens (i) bij wet is voorzien, (ii) een legitiem doel dient en (iii) of de verwerking noodzakelijk is in een democratische samenleving. Daarnaast moeten de beoogde verwerkingen die voortvloeien uit het wetsvoorstel proportioneel (de mate waarin de inbreuken in verhouding staan tot het belang/noodzaak) en subsidiair zijn (de vraag of de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze kunnen worden bereikt (iv). Deze factoren zijn in de MvT bij het wetsvoorstel uitgewerkt in paragraaf 3.6.3. In de kaders hieronder volgt een weergave van wat hierover in de MvT wordt uiteengezet. Vervolgens volgt een voor de DPIA relevante reflectie.

(i) Bij wet voorzien

> *Het wetsvoorstel voorziet in grondslagen voor het verwerken van persoonsgegevens door de defensieonderdelen en beperkt de bescherming van de betrokkene. Daarmee voorziet het wetsvoorstel in een wettelijke basis. De Grondwet vereist dat deze beperkingen bij of krachtens een wet in formele zin worden gesteld. Uit rechtspraak van het EHRM volgt dat deze wettelijke basis voldoende precies, duidelijk, voorzienbaar en toegankelijk moet zijn.[51] Binnen het domein van nationale veiligheid wordt daarbij aan de voorzienbaarheid een andere invulling gegeven dan voor andere algemene belangen. Een wettelijke basis moet daartoe voldoende duidelijk zijn over de omstandigheden en de voorwaarden waaronder een overheidsorgaan bevoegd is om gegevens te verwerken.[52]*
>
> *Dit wetsvoorstel voorziet voor een groot aantal gegevensverwerkingen in een expliciete wettelijke basis van die verwerkingen die een inbreuk kunnen maken op de persoonlijke levenssfeer. Daarbij wordt zoals eerdergenoemd een onderscheid gemaakt tussen drie categorieën van activiteiten. De verwerking van persoonsgegevens die bij deze activiteiten plaats kan vinden is gebonden aan het doel en gebonden aan voorwaarden. Bij die verwerkingen wordt ook meegegeven onder welke omstandigheden persoonsgegevens stelselmatig verwerkt en bewaard kunnen worden. Het uitgangspunt in dit wetsvoorstel is dat dit slechts in uitzonderlijke omstandigheden mogelijk is.*

Het wetsvoorstel voorziet in een wettelijke basis voor het verwerken van persoonsgegevens en het beperken van rechten van de betrokkene, voor zover dit noodzakelijk is voor het verrichten van gereedstellingsactiviteiten die worden uitgevoerd door de krijgsmacht en van de defensieonderdelen. Deze verwerkingsgrondslagen hebben betrekking op de operationele, personele en materiële gereedstelling en de geoefendheid van het militair vermogen in de informatieomgeving. Ook zijn er specifieke grondslagen voor de verwerking

[51] EHRM 26 april 1979, ECLI:CE:ECHR:1979:0426JUD000653874 (Sunday Times/Verenigd Koninkrijk), par. 49 en EHRM 25 maart 1983, ECLI:CE:ECHR:1983:0325JUD000594772 (Silver e.a./Verenigd Koninkrijk), par. 87.
[52] EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa/Zweden*), par. 247.

van persoonsgegevens bij 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. Tot slot zijn er gegevensverwerkingen in het kader van de gezondheid van militairen.

Het wetsvoorstel is voldoende duidelijk over de omstandigheden en de voorwaarden waaronder Defensie bevoegd is om persoonsgegevens te verwerken. Hiermee voldoet het wetsvoorstel aan de vereisten die uit de Grondwet en de rechtspraak van het EHRM voortvloeien ten aanzien van de voorzienbaarheid. Daarnaast maakt de Wodg als wet in formele zin, gepaard met de MvT, de afweging die ten grondslag ligt aan de inzet van de benodigde bevoegdheden transparanter en beter voorzienbaar voor betrokkenen.

(ii) Legitiem doel

De verwerking van persoonsgegevens door de defensieonderdelen dient de daadwerkelijke en stelselmatige gereedheid van de krijgsmacht en daarmee het militair vermogen van de krijgsmacht.[53] De krijgsmacht heeft op grond van artikel 97, eerste lid, van de Grondwet in samenhang met artikel 5 van het Noord-Atlantisch Verdrag als taak om het Koninkrijk en het bondgenootschappelijk grondgebied te beschermen. Een belangrijk onderdeel van de bescherming is de afschrikking, waarmee voorkomen kan worden dat het tot inzet van de krijgsmacht komt en een verdergaande inbreuk op de persoonlijke levenssfeer wordt voorkomen. Hiervoor is vereist dat de krijgsmacht gereed is voor inzet, zoals ook door artikel 3 van het Noord-Atlantisch Verdrag wordt verplicht. De gereedheid van de krijgsmacht is van vitaal belang om het militair vermogen van de krijgsmacht te waarborgen.

Om gereed te zijn dienen gereedstellingsactiviteiten verricht te worden. Er bestaat een dwingende maatschappelijke behoefte om deze gereedstellingsactiviteiten mogelijk te maken gezien de toegenomen frequentie en intensiteit van conflicten in de buurt van Europa zoals is toegelicht in paragraaf 1.1 van de toelichting. Dit ziet op activiteiten ten behoeve van de personele en materiële gereedheid en de geoefendheid. Deze activiteiten vinden plaats in de fysieke leefomgeving, maar ook online, waarbij bedoeld en onbedoeld persoonsgegevens verwerkt worden. Als onderdeel van de gereedheid van de krijgsmacht is ook vereist dat zij beschikt over informatie over actoren en factoren in potentiële inzetgebieden en dreigingen van buitenaf. Die informatiepositie heeft als doel om te zorgen dat de krijgsmacht veilig ingezet wordt (personele veiligheid) en proportioneel en doeltreffend handelt. Het is in de operationele omgeving van essentieel belang om een onderscheid te maken tussen gewone burgers en militairen of andere gevaarlijke actoren en tussen civiele infrastructuur en militaire doelwitten. Hiermee moet onnodig leed worden voorkomen bij de inzet van de krijgsmacht. Ten slotte moeten de netwerk- en informatiesystemen van de defensieonderdelen, militaire objecten en het defensiepersoneel te allen tijde bewaakt en beveiligd worden. Dit is deels een zelfstandig vitaal belang, waarbij eveneens de inzetgereedheid van de krijgsmacht en het afschrikwekkend effect daarvan ernstig bedreigd kunnen worden.

[53] Onder het EVRM valt een rechtvaardiging op grond van defensiedoeleinden onder de rechtvaardigingsgrond 'nationale veiligheid', zie: EHRM 27 september 1999, ECLI:CE:ECHR:1999:0927JUD003141796 (Lustig-Prean en Beckett/Verenigd Koninkrijk), par. 87.

In het wetsvoorstel en in de MvT wordt uitgewerkt voor welk doel de specifieke gereedstellingsactiviteiten, en de daarmee gepaard gaande verwerkingen van persoonsgegevens, noodzakelijk zijn. Het wetsvoorstel definieert de gereedheid van de krijgsmacht als een zelfstandig vitaal belang. Onderbouwd wordt dat de verplichting tot de gereedheid volgt uit zowel nationale als internationale verplichtingen, waarin de bescherming van het Koninkrijk en het bondgenootschappelijk grondgebied als taak voor de krijgsmacht is geformuleerd. Aldus wordt in het wetsvoorstel en de MvT voldoende onderbouwd welk legitiem doel de verwerkingen van persoonsgegevens en mogelijke inbreuken op de persoonlijke levenssfeer dienen.

(iii) Noodzakelijk in een democratische samenleving

Het waarborgen van de gereedheid van de krijgsmacht is in het licht van het vitale belang van de gereedheid van de krijgsmacht noodzakelijk in een democratische samenleving. Daartoe is vereist dat er een balans bestaat tussen het algemene publieke belang en de individuele belangen en grondrechten van burgers. Deze balans wordt ingevuld aan de hand van de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit.

De verwerkingen in deze wet kunnen slechts plaatsvinden indien dit ook noodzakelijk is voor het specifieke doel. Deze doelen zijn verbonden aan de grondwettelijke taak uit artikel 97 van de Grondwet en bondgenootschappelijke verplichtingen (zie nader paragraaf 1.1) waartoe de krijgsmacht daadwerkelijk en stelselmatig gereed moet zijn. Bij de activiteiten die plaatsvinden ten behoeve van de personele en materiele gereedheid en de geoefendheid kunnen persoonsgegevens worden verwerkt. Die verwerking vindt alleen plaats als dit noodzakelijk is en daarbij wordt de inbreuk op de persoonlijke levenssfeer voor zover mogelijk beperkt. Dit hangt deels samen met de gereedstellingssystematiek (paragraaf 1.3), waarbij gereedstellingsactiviteiten pas op het vierde niveau en bij de certificering in de openbare ruimte plaatsvinden. Daarmee wordt zover als mogelijk beoogt om de gegevensverwerkingen tot het strikt noodzakelijk te beperken. Daarnaast vinden deze activiteiten in veel gevallen niet plaats om persoonsgegevens te verwerken, maar zijn deze bijvangst van de activiteit. Persoonsgegevens worden dan verwijderd en terstond vernietigd. In een aantal gevallen vinden activiteiten plaats die wel gericht zijn op het verwerken van persoonsgegevens, bijvoorbeeld bij het gereedstellen van cyberspecialisten. Ook hierbij gelden waarborgen zoals het uitgangspunt dat die gegevens niet worden bewaard en als dat wel het geval is dat deze worden geanonimiseerd of gepseudonimiseerd om te bewerkstellingen dat de inbreuk op de persoonlijke levenssfeer beperkt blijft.

De gegevensverwerkingen die plaatsvinden ten behoeve van de informatiepositie kunnen onder omstandigheden een grotere inbreuk op de persoonlijke levenssfeer meebrengen. Als belangrijkste waarborg is dat alleen in specifieke omstandigheden gegevens verwerkt mogen worden met als doel om onderzoek te doen naar die persoon. In alle andere gevallen worden gegevens niet persoonsgericht worden verzameld. Voor de specifieke gevallen waar dit wel mag, is een aanwijzing dan wel de goedkeuring van de Minister van Defensie vereist. Met betrekking tot de relevante publieke organen en civiele actoren die de krijgsmacht kunnen ondersteunen en de te beschermen personen is als beperking gesteld dat deze personen niet stelselmatig gemonitord mogen worden. In aanvulling daarop wordt waar mogelijk

ook samengewerkt met bondgenoten en de diensten om te voorkomen dat er een dubbele inbreuk plaatsvindt. Daartoe vindt er ook afstemming plaats met de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). In verband met de onvoorspelbaarheid van de inzet, de inhoud van de tactische en operationele informatie en de efficiency dient de krijgsmacht zelfstandig deze kennis te kunnen vergaren.

Bij het bewaken en beveiligen en daaraan verbonden gegevensverwerkingen vinden alleen plaats als deze voor het specifieke doel noodzakelijk zijn. Als belangrijkste waarborg geldt dat persoonsgegevens niet verzameld mogen worden met behulp van een technisch hulpmiddel om een persoon stelselmatig te monitoren. Daarnaast geldt dat als wel beoogd wordt om een persoon nader te identificeren en daartoe persoonsgegevens te verwerken die afweging zorgvuldig gedaan moet worden, rekening houdend met de proportionaliteit en subsidiariteit. Bij het beveiligen van de netwerk- en informatiesystemen is waar mogelijk aangesloten bij de systematiek die ook geldt voor het beveiligen van kritieke, essentiële en belangrijke entiteiten.

In de MvT wordt omschreven dat de verwerking van persoonsgegevens enkel plaatsvindt voor zover noodzakelijk, waarbij de inbreuk op de persoonlijke levenssfeer voor zover mogelijk wordt beperkt. Hiervoor worden verschillende factoren benoemd waarmee dit in het wetsvoorstel wordt bewerkstelligd. In de proportionaliteits- en subsidiariteitsafweging hierna worden deze factoren betrokken.

(iv) *Proportionaliteit en subsidiariteit*

Subsidiariteit
Het *beginsel van subsidiariteit* brengt mee dat de beperking van het grondrecht van de bescherming van de persoonlijke levenssfeer niet rechtmatig is als het daarmee beoogde doel ook kan worden bereikt op een wijze die het grondrecht niet of in minder mate beperkt en daarmee voor de betrokkenen minder nadelige effecten heeft. Voorafgaand aan de ontwikkeling van dit wetsvoorstel zijn verschillende strategieën overwogen, zoals het verbeteren van de bestaande kaders en het ontwikkelen van tijdelijke organisatorische en technische maatregelen om de doelen, zoals ook geformuleerd in het wetsvoorstel, te kunnen bereiken. Deze boden echter geen structurele oplossing voor het verzekeren van een daadwerkelijke en stelselmatige gereedheid van het militair vermogen van de krijgsmacht. Dat het bestaande juridische kader knelpunten oplevert bij de gereedheid van de krijgsmacht werd in meerdere adviezen en onderzoeksrapporten geconstateerd (de commissie Brouwer[54], EIFFEL[55], NLDA[56], WRR[57] en de AIV[58]). Het wetsvoorstel biedt structurele bevoegdheden met structurele waarborgen. Bovendien maakt de Wodg als formele wet, gepaard met de uitvoerige MvT, de afweging die ten grondslag ligt aan de inzet van de benodigde bevoegdheden

[54] 'Grondslag gezocht' Grondslag gezocht - Onderzoekscommissie Land Information Manoeuvre Centre (LIMC) van de commissie Brouwer (https://www.rijksoverheid.nl/documenten/rapporten/2023/01/13/rapport-onderzoekscommissie-brouwer-naar-het-land-information-manoeuvre-centre-limc)
[55] EIFFEL B.V., Onderzoek AVG – Ministerie van Defensie, juli 2022.
[56] Ducheine, Paul, Peter Pijpers, Marten Zwanenburg, Rapport Tanden voor de Leeuw, Een voor haar doel en op haar taak berekende krijgsmacht in de informatie-omgeving, (NLDA-WSRC, 4-4-2024). Aangeboden via Kamerstukken II, 2024-25, 33763, nr. 158
[57] Wetenschappelijke Raad voor Regeringsbeleid (WRR), Nederland in een fragmenterende wereldorde (rapport nr. 109), 2024.
[58] Adviesraad Internationale Vraagstukken (AIV), "Hybride dreigingen en maatschappelijke weerbaarheid." (AIV-advies 126), 2024. Zie ook de kabinetsreactie op het AIV-advies (Kamerstuk 30 821, nr. 250).

transparanter en beter voorzienbaar voor betrokkenen dan de huidige werkwijze die gebaseerd is op een meer versnipperd juridisch kader. Uit deze voorgeschiedenis volgt dat dit wetsvoorstel verenigbaar is met het beginsel van subsidiariteit.

Proportionaliteit
Bij de beoordeling van het *proportionaliteitsbeginsel* gaat het om de vraag of de maatregel evenredig (proportioneel) is aan het doel dat daarmee kan worden bereikt. De legitimering van het doel van het wetsvoorstel is in de MvT voldoende onderbouwd. De vraag is of de beperking van het grondrecht op privacy en het doel dat met de Wodg wordt beoogd met elkaar in balans zijn. Daarvoor is onder meer van belang hoe groot de inbreuk is en welke waarborgen daartegenover staan. In de Wodg zijn in artikel 4.2 de algemene waarborgen voor betrokkenen opgenomen. Daarnaast bevat artikel 4.7 lid 3 tot en met lid 7 (informatiepositie) nadere waarborgen voor de gerichte vergaring van kennis over specifieke personen. Waar de inbreuk groter is, worden in het wetsvoorstel aldus aanvullende en specifieke waarborgen geboden.

Ten aanzien van de bijzondere en strafrechtelijke persoonsgegevens zijn aanvullende waarborgen gesteld (artikel 4.5). Daarmee biedt het wetsvoorstel voldoende waarborgen ten behoeve van de verwerking van bijzondere- en strafrechtelijke categorieën van persoonsgegevens.

Wat betreft het optreden in het elektromagnetisch spectrum (artikel 4.7 lid 2 sub c) wordt een onderscheid gemaakt tussen de inhoud van de communicatie en de metadata. Dit laatste mag wel worden verwerkt, waaronder ook mogelijke persoonsgegevens in metadata. Dit heeft een impact op de proportionaliteit van het wetsvoorstel, aangezien aanvullende waarborgen voor dit deel ontbreken en betrokkenen mogelijk een risico lopen. Voorts wordt in de Wodg (artikel 4.11 lid 3) ook aangegeven dat bij gegevensverwerkingen in het kader van bescherming van militaire objecten en defensiepersoneel via eigen waarneming er geen technische hulpmiddelen worden gebruikt met doel om communicatie af te tappen, te ontvangen, op te nemen of af te luisteren, dan wel om een geautomatiseerd werk binnen te dringen.

Ten aanzien van de enquête in het kader van werving van militair Defensiepersoneel is dit een begrijpelijke behoefte gegeven de huidige geopolitieke dreigingen alsmede het tekort aan Defensiepersoneel. Defensie heeft de ambitie gesteld om een gevulde organisatie te zijn, die schaalbaar kan meebewegen met het actuele dreigingsbeeld. Indien het doel is bereikt, is het van belang om het gebruikte middel (enquête) te heroverwegen en/of aan te passen. Het gebruikte middel moet altijd in verhouding blijven staan tot de inbreuk die wordt gemaakt op de rechten en vrijheden van betrokkenen.

Daarnaast is bij een enquête de kans, zeker bij open (vrije) tekstvelden, aanwezig dat mensen meer informatie dan relevant verstrekken, waardoor Defensie mogelijk onnodig veel informatie vergaart, waaronder bijzondere persoonsgegevens. Het gaat hier om de antwoorden op vragen opgenomen over fysieke en mentale gezondheid. Om van een proportioneel middel te kunnen blijven spreken is van belang dat het aantal verwerkte gegevens tot het voor het doel noodzakelijke beperkt blijft. Het is bijvoorbeeld nadrukkelijk niet de bedoeling dat de enquête (in bepaalde mate) de rol van een keuring in de zin van de Wet op de medische keuringen overneemt. Door het vrijwillige karakter van de enquête wordt er ook tegemoetgekomen aan eventuele

gewetensbezwaren[59]. Tot slot geldt de AVG onverkort ten aanzien van deze enquête, waardoor betrokkenen hun rechten onbeperkt kunnen uitoefenen.

Er zijn nog meer factoren die betrokken kunnen worden in de proportionaliteitsafweging. Een aantal daarvan is in de MvT benoemd om de noodzakelijkheid van de verwerkingen van persoonsgegevens in een democratische samenleving te onderbouwen. Genoemd wordt dat de verwerkingen beperkt worden tot noodzakelijke en ook dat veel activiteiten niet als doel hebben om persoonsgegevens te verwerken, zodat de gegevens in die gevallen als bijvangst worden verwijderd en terstond worden vernietigd. De gereedstellingsactiviteiten die wel gericht zijn op het verwerken van persoonsgegevens zijn met waarborgen omkleed en zodra de inbreuk groter is (zoals bij gerichte vergaring ten aanzien van personen) gelden er aanvullende waarborgen. Voorts is de gereedstellingssystematiek voor de afweging van de proportionaliteit van belang. De MvT beschrijft die systematiek als volgt:

> *Het gereedstellingsproces is voor elk operationeel commando anders ingericht als gevolg van de specifieke karakteristieken en eigenschappen van de eenheden en het operationeel domein waarin moet worden opgetreden en de (wapen)systemen die daarbij worden gebruikt. Waar passend wordt in dat proces gebruik gemaakt van een gereedstellingssystematiek met verschillende gereedstellingsniveaus.[60] Die systematiek houdt in dat het opleiden, trainen en oefenen van militairen op vier niveaus plaatsvindt en afgesloten wordt met een certificering.[61] Binnen die vier niveaus wordt bij de eerste drie niveaus in een besloten omgeving getraind en alleen bij het vierde niveau wordt gebruik gemaakt van de publieke ruimte. Op het eerste niveau wordt op lokaal niveau getraind. Op het tweede niveau wordt getraind door middel van nabootsing, zoals een cyberrange. En op het derde niveau wordt getraind door middel van een synthetisch nagebootste omgeving. Op het vierde niveau wordt in de openbare ruimte getraind, waarbij zoveel mogelijk waarborgen zijn ingebouwd om de risico's voor derden te beperken. Een eenheid sluit het gereedstellingsproces af met een certificeringsoefening, waarbij het behalen van de certificering betekent dat de eenheid inzetgereed is.*
>
> *Dit gereedstellingsproces moet ertoe leiden dat eenheden gereed zijn om hun taken uit te kunnen voeren, dan is deze eenheid operationeel gereed. Daartoe is vereist dat deze eenheid voldoet aan de normen van personele- en materiele gereedheid en geoefendheid.*

Deze systematiek is in zichzelf een instrument om de proportionaliteit te kunnen beïnvloeden. In de MvT werd ter onderbouwing van de noodzakelijkheid in een democratische rechtsstaat beschreven dat gereedstellingsactiviteiten pas op het vierde niveau en bij de certificering in de openbare ruimte plaatsvinden, waarmee wordt beoogd om de gegevensverwerkingen en inbreuken op het grondrecht van privacy steeds tot het strikt noodzakelijke te beperken.

---

[59] Zoals bedoeld in artikel 99 Grondwet en nader uitgewerkt in de Wet gewetensbezwaren militaire dienst.

[60] Zo verloopt dit momenteel bij het Commando zeestrijdkrachten en het Commando landstrijdkrachten.

[61] P. Ducheine, P. Pijpers & M. Zwanenburg, Tanden voor de Leeuw – Een voor haar doel en op haar taak
berekende krijgsmacht in de informatie-omgeving, april 2024, gepubliceerd in: *Kamerstukken II* 2024/25,
33 763, nr. 158, p. 43-45.

Concluderend: het wetsvoorstel biedt de ruimte voor potentieel vergaande inbreuken op de persoonlijke levenssfeer. Deze inbreuken zijn mede afhankelijk van de wijze waarop daarvoor nadere regels worden gesteld bij AMvB en de wijze van uitvoering van de bevoegdheden. Het wetsvoorstel voorziet, als tegenhang voor de potentieel vergaande inbreuken, in een adequaat waarborgen- en toezichtstelsel. In de MvT wordt hierover het volgende beschreven.

> *Daarnaast zijn in dit wetsvoorstel algemene waarborgen opgenomen, waaronder regels over de bewaartermijnen en specifieke voorwaarden bij de verwerking van bijzondere categorieën van persoonsgegevens en persoonsgegevens van strafrechtelijke aard. In aanvulling daarop zijn per verwerkingsgrondslag aanvullende waarborgen opgenomen. Deze waarborgen hebben onder andere betrekking op de wijze van gegevensverzameling, de gegevensbronnen die gebruikt kunnen worden en specifieke beperkingen van de verwerkingsdoeleinden.*
>
> *Voor de verstrekking van gegevens aan derden is in dit wetsvoorstel een gesloten verstrekkingsregime opgenomen. Daarbij gelden voor verstrekkingen aan het buitenland aanvullende waarborgen, zoals een vertrouwelijkheidsbeoordeling en belangenafweging.*
>
> *Voor de rechten van betrokkene wordt voorzien in een eigen regime van rechten van betrokkene, waarbij rekening wordt gehouden met de specifieke context waarin de gegevensverwerkingen in het kader van deze wet plaatsvindt. In die context voorziet dit wetsvoorstel in een mededeling van de verwerking van persoonsgegevens en een recht op kennisneming van de verwerkte persoonsgegevens van de betrokkene.*

Voorts zal conform de reguliere praktijk bij het daadwerkelijk gebruik van de bevoegdheden waar het wetsvoorstel een grondslag voor biedt per casus een toets op proportionaliteit en subsidiariteit moeten plaatsvinden.

15. Rechten van betrokkenen

De Wodg legt, in het kader van de daadwerkelijke en stelselmatige militaire gereedheid, specifieke beperkingen op aan de rechten van betrokkenen zoals vastgelegd in Hoofdstuk III van de AVG. Hiermee wordt het bestaande uitzonderingsregime in artikel 3 UAVG en de Regeling Gegevensbescherming Militaire Operaties (RGMO) verbreed naar de activiteiten in het kader van gereedstelling.

Paragraaf 4.6 (artikelen 4.13 t/m 4.16) van de Wodg geeft een eigen kader voor de rechten van betrokkenen, waarbij wordt voorzien in een verplichte, publieke mededeling van de Minister indien persoonsgegevens zullen worden verwerkt voor a) het voorbereiden, onderhouden en verbeteren van de geoefendheid van de defensieonderdelen, b) het onderhouden en vernieuwen van materieel of militaire objecten of c) het werven, opleiden en trainen van militaire ambtenaren en dienstplichtigen.

Het kader bevat de volgende rechten:

- **Recht op informatie en inzage**
  Artikel 4.13 van de Wodg legt beperkingen op aan het recht op informatie en inzage als de bekendmaking van dergelijke informatie de vertrouwelijkheid van defensieactiviteiten kan schaden. Er een specifieke regeling inzake kennisneming voorzien; artikel 4.14 introduceert een recht op kennisneming, vergelijkbaar met de regeling onder de Wiv 2017. Het recht op kennisneming van persoonsgegevens komt toe aan de betrokkene zelf. Over dit recht wordt in de MvT, in de artikelsgewijze toelichting bij artikel 4.14, het volgende geschreven:

  > *Het recht op kennisneming is een aanvullende waarborg bovenop de in artikel 4.3 gestelde bewaartermijnen van al dan niet gepseudonimiseerde persoonsgegevens. Aangezien persoonsgegevens die niet langer noodzakelijk zijn voor het doel waarvoor ze zijn verwerkt worden vernietigd, zal het recht op kennisneming niet vaak hoeven worden ingezet. In veel gevallen zal een aanvraag worden afgewezen omdat de gegevens waar de aanvraag betrekking op heeft niet meer aanwezig zijn.*

- **Recht op correctie en gegevenswissing**
  Betrokkenen hebben de mogelijkheid om onjuistheden of onvolledigheden te melden via een verklaring zoals bepaald in artikel 4.15 van de Wodg. Deze verklaring wordt toegevoegd aan de verwerkte persoonsgegevens en biedt een (materieel) alternatief voor het recht op correctie en gegevenswissing.

- **Recht van bezwaar en beperking van verwerking**
  Artikel 4.16 bepaalt de omstandigheden waaronder een verzoek om inzage of correctie kan worden afgewezen, bijvoorbeeld wanneer dit de nationale veiligheid in gevaar zou brengen. Deze weigeringsgronden zijn in lijn met de Wet open overheid (Woo) geformuleerd.

- **Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming**
  Geautomatiseerde besluitvorming wordt toegestaan indien noodzakelijk voor militaire operaties en wanneer deze geen wezenlijke schade toebrengt aan de rechten van betrokkenen.

Waarborgen en handelingsperspectief
Op grond van de AVG zijn de Functionaris voor Gegevensbescherming en de Autoriteit Persoonsgegevens verantwoordelijk voor het interne en externe toezicht op de naleving van dit wetsvoorstel.

- **Klachtenprocedure bij de FG**
  Betrokkenen behouden het recht om een klacht in te dienen bij de FG. Nieuwe normenkaders binnen Defensie bieden duidelijkheid over welke informatie kan worden verstrekt en hoe met klachten wordt omgegaan (artikel 38, lid 4 AVG).
- **Recht om klacht of beroep in te stellen (artikel 4.13, g)**
  Betrokkenen kunnen een klacht indienen bij de Autoriteit Persoonsgegevens (artikel 77 AVG) en in beroep gaan tegen beslissingen van de Minister van Defensie als verwerkingsverantwoordelijke (artikel 79 AVG).

C Beschrijving en beoordeling risico's voor de betrokkenen

16. Risico's voor betrokkenen

Er zijn diverse risico's te identificeren bij verwerkingen van persoonsgegevens die voortvloeien uit het wetsvoorstel. Onderstaande risico's zijn geformuleerd op een hoog abstractieniveau om een breed beeld te geven van de potentiële risico's met betrekking tot de rechten en vrijheden van betrokkenen.

- **Verlies van controle over persoonsgegevens door onduidelijke taakafbakening tussen (overheids-)instanties**
  Het risico bestaat dat persoonsgegevens van betrokkenen zonder hun medeweten door Defensie worden verwerkt. De redelijke privacy-verwachting kan in het geding komen doordat de taken, verantwoordelijkheden en bevoegdheden tussen overheidsinstanties zoals Politie, Algemene Inlichtingen- en veiligheidsdienst (AIVD), Koninklijke Marechaussee (KMar), Krijgsmacht en MIVD overlappen of onduidelijk zijn onderscheiden. Daadwerkelijke overlap of schurende juridische regimes, maar ook onbekendheid of onwetendheid bij het grote publiek over de samenwerkingen en afbakeningen van taken, verantwoordelijkheden en bevoegdheden, kunnen leiden tot gevoelens van machteloosheid, waardoor betrokkenen controle/zeggenschap over hun persoonsgegevens en privacy verliezen alsook verlies van vertrouwen in de overheid.

- **Ongeautoriseerd gebruik van persoonsgegevens door gebrek aan regels (*scope creep*)**
  Het risico bestaat dat persoonsgegevens zonder voldoende beperkingen worden verzameld en gedeeld. Er kunnen onvoorziene verwerkingen van persoonsgegevens plaatsvinden, zonder duidelijke sturing, wanneer bevoegdheden breder worden toegepast dan bedoeld en het principe van doelbinding onvoldoende voor ogen wordt gehouden, bijvoorbeeld wanneer persoonsgegevens relevant kunnen zijn voor de verschillende taakgebieden ('geoefendheid en gereedheid,' 'informatiepositie,' en 'bewaken en beveiligen'). Gegevensverwerkingen die onvoorzien zijn of de bevoegdheid te buiten gaan, kunnen plaatsvinden binnen Defensie of door (inter)nationale samenwerking, onder meer wanneer persoonsgegevens worden verstrekt aan partijen met meer of andere bevoegdheden of minder strenge privacybescherming, omdat ze bijvoorbeeld buiten het toepassingsgebied van de AVG vallen. Dit kan leiden tot ongeautoriseerd of ongewenst gebruik door onbevoegde organisatieonderdelen of partijen. Hun specifieke acties kunnen de privacy en veiligheid van betrokkenen in gevaar brengen. Betrokkenen kunnen zorgen hebben over wie toegang heeft tot hun persoonsgegevens en de mogelijke gevolgen daarvan.

- **Schade door inadequaat gegevensbeheer en gebrekkige beveiliging (incl. incident management)**
  Het risico bestaat dat de mogelijkheid om persoonsgegevens lang te bewaren in combinatie met ontoereikend beveiligde IT-systemen kan leiden tot onbehoorlijke opslag en behandeling van persoonsgegevens. Dit kan de kans op inbreuken (datalekken) vergroten, die vervolgens kunnen resulteren in, bijvoorbeeld, verlies van controle over persoonsgegevens of identiteitsdiefstal of -fraude of andersoortige nadelen voor de persoon in kwestie. Ook kunnen problemen in datakwaliteit en -management leiden tot foutieve analyses en beslissingen. Er kunnen concrete gevaren en directe financiële/persoonlijke schades voortvloeien uit inadequaat gegevensbeheer. Het risico bestaat ook dat er oneigenlijk lang persoonsgegevens worden bewaard (zie artikel 4.3 lid 2), aangezien de bewaartermijn telkens voor ten hoogste een jaar – via een daartoe

strekkend verzoek aan de minister – kan worden verlengd. Dit zal eveneens voor uitvoeringsproblemen kunnen zorgen.

- **Ongewenste profilering en discriminatie door geautomatiseerde systemen**
  Het risico bestaat dat betrokkenen systematisch worden blootgesteld aan vooroordelen en discriminatie door inherente bias in geautomatiseerde systemen en profileringstechnieken. Dit kan gebeuren wanneer de werking van algoritmen niet transparant is. In dergelijke situaties kunnen vooroordelen leiden tot ongelijkheid in behandeling in gelijke gevallen. Als hierbij de rechten van betrokkenen niet voldoende worden beschermd, zou dat het vertrouwen in deze technologieën kunnen ondermijnen.

- **Beperkte mogelijkheid tot uitoefening van rechten en toegang tot juridische bescherming door gebrek aan transparantie**
  Het risico bestaat dat de effectieve rechtsbescherming van betrokkenen in gevaar komt. Het beperken van de rechten van betrokkenen en de vertrouwelijkheid van Defensieactiviteiten (beperkte transparantiemogelijkheden) kunnen het voor betrokkenen moeilijk maken om beroep te doen op hun rechten. Wanneer betrokkenen hun persoonsgegevens bijvoorbeeld niet kunnen inzien en rectificeren kan de wijze van verwerking van persoonsgegevens niet worden geverifieerd en eventueel in een procedure aanhangig worden gemaakt. Dit heeft tot gevolg dat de effectieve toegang tot rechtsmiddelen voor betrokkenen beperkt is en kan tevens leiden tot een verlies van vertrouwen in de overheid.

- **Verandering van gedrag door monitoring (*chilling* effect)**
  Het risico bestaat dat betrokkenen zich gedwongen voelen hun gedrag aan te passen uit angst voor monitoring door Defensie, zowel in de publieke ruimte als op de werkvloer. Percepties over gevolgd kunnen worden of de daadwerkelijk uitvoering van gereedstellingsactiviteiten waarbij betrokkenen gevolgd kunnen worden in de fysieke en virtuele omgeving, kunnen de vrijheid van handelen en de vrijheid van meningsuiting beperken en de beleving van veiligheid van betrokkenen schaden. Inperkingen van persoonlijke vrijheid en autonomie (of wanneer dat als zodanig wordt ervaren) hebben impact op een democratische rechtstaat en de samenleving als geheel.

- **Te ruime verwerking van persoonsgegevens in het kader van de enquête**
  Het risico bestaat dat mensen, wanneer er niet gestuurd wordt op de gewenste (hoeveelheid) informatie, meer informatie dan nodig aan Defensie verstrekken. Ook het (te) lang bewaren van de vergaarde informatie is een risico. Hier betreft hier mogelijk ook om gegevens omtrent gezondheid (antwoorden op vragen over fysieke en psychologische belastbaarheid).

Deze DPIA beschrijft risico's voor betrokkenen die voortvloeien uit het wetsvoorstel. Daarnaast zullen er risico's zijn die samenhangen met de *implementatie* van de in het wetsvoorstel opgenomen waarborgen die samenhangen met de *uitvoering* van de Wodg. Hierbij valt te denken aan gevolgen door een tekort aan capaciteit (kwantitatief en kwalitatief), beperkte prioritering en knelpunten voortkomend uit de volwassenheidsniveaus op het gebied van datamanagement, compliance- en privacyprocessen. Het is van belang de implementatie- en uitvoeringsrisico's mee te nemen in het verdere wetgevingsproces met (reguliere) toetsingsprocessen, gedurende de implementatie en tijdens periodieke evaluaties.

D Maatregelen en restrisico's

17. Maatregelen

Diverse maatregelen kunnen bijdragen aan het beperken van de geïdentificeerde risico's voor betrokkenen bij verwerkingen van persoonsgegevens. Dit hoofdstuk bevat een inventarisatie van die maatregelen, geclusterd aan de hand van vijf pijlers (strategie, mensen, processen, data en technologie), om een gestructureerd en samenhangend overzicht te bieden. Bij de uitvoering van de Wodg is tevens aandacht nodig voor bredere organisatorische aspecten die de effectieve naleving en bescherming van persoonsgegevens ondersteunen. Hiervoor zijn bestaande (beleids)programma's en innovatietrajecten, zoals het op orde brengen van de informatiehuishouding en het verstevigen van de privacyorganisatie.

STRATEGIE
De maatregelen onder strategie richten zich op het verduidelijken en vaststellen van verantwoordelijkheden ten behoeve van de doelbinding. Dat is van belang voor het minimaliseren van risico's als gevolg van onduidelijke bevoegdheden en verwerkingen van persoonsgegevens zonder specifieke, expliciete en legitieme reden.

- **Codificatie van taken en verantwoordelijkheden**
  Door verantwoordelijkheden en bevoegdheden van Defensieonderdelen verder in te kaderen in de (communicatie over de) Wodg en in toekomstige AMvB's, wordt verwarring over welke instanties welke gegevensverwerkingen uitvoeren, verminderd. Dit helpt bij het afbakenen van taken en het voorkomen van ongewenste gegevensverwerkingen. Defensie zal voldoende capaciteit vrij moeten maken voor de interdepartementale verhoudingen, afstemming en implementatie van deze codificaties.

- **Besturing en verantwoordelijkheidstoewijzing**
  De Minister zal de reikwijdte van de nieuwe bevoegdheden formuleren ten behoeve van toekomstige orders aan de voorkant van het proces (zoals in oefenorders), waardoor de operationele eenheden nieuwe bevoegdheden op een gecontroleerde en afgebakende wijze kunnen toepassen. Het aanstellen van specifieke compliance- en privacyfunctionarissen voor de Wodg (binnen de huidige privacy- en compliance organisatie van Defensie) kan de nodige begeleiding bieden bij het werken met nieuwe bevoegdheden en toepassen van privacy-beginselen op het tactische/operationele niveau. Via interne en externe controlemechanismes (audits en toezicht) kunnen de belangen van betrokkenen worden vertegenwoordigd en verwachtingen worden verduidelijkt. Door regelmatige onderzoeken en de opvolging van aanbevelingen die daaruit volgen, kan worden gezorgd dat gegevensverwerkingen voldoen aan de gestelde doelen en dat persoonsgegevens niet onnodig (en/of te lang) bewaard worden.

- **(Beleids)afspraken en richtlijnen voor gegevensverstrekking**
  Nationale en internationale beleidsafspraken en duidelijke richtlijnen voor gegevensverstrekking helpen de privacy van individuen te waarborgen en te voorkomen dat persoonsgegevens ongeoorloofd worden gedeeld. Er zijn kaders nodig die bepalen welke persoonsgegevens, waar Defensie over beschikt, aan welke (nationale of internationale) partijen verstrekt kunnen worden en welke waarborgen daarbij nodig zijn. Daarbij is ook aandacht nodig voor het stellen van voorwaarden aan de mogelijkheid voor een derde partij om opbrengsten van de ene opdracht te gebruiken voor een

andere opdracht.

- **Communicatie(plannen) en betrokkenheid**
  Door potentiële zorgen over gegevensverwerkingen proactief te verantwoorden middels politieke en maatschappelijke betrokkenheid en transparantie, wordt het vertrouwen van individuen versterkt. Het organiseren van voorlichting aan de samenleving over het doel en de reikwijdte van bevoegdheden en gegevensverwerkingen kan echter uitdagend zijn gezien de vertrouwelijkheid van deze informatie. Het faciliteren van klachten- en bezwaarprocedures via de FG en de AP, rechter en ombudsman kan zorgen voor de nodige (juridische) middelen voor de uitoefening van rechten en zorgen door individuen.

MENSEN
Door te investeren in training en voorlichting wordt een cultuur van bewustwording en ethische omgang met persoonsgegevens bevorderd. Dit helpt het risico van onbewuste privacy schendingen te minimaliseren.

- **Gedrag en bewustwording**
  Gerichte trainingen over datageletterdheid, gegevensbeheer, en privacy/security/archiving-by-design helpen personeel zich bewust te zijn van hun rol in het naleven van gegevensbescherming. Dit vermindert de kans op ongeautoriseerd gebruik en onethische profilering. Laagdrempelige communicatiekanalen voor interne vragen en klachten zorgen voor duidelijkheid, waardoor angst voor gevolgd te worden op de werkvloer en misverstanden worden verminderd.

PROCESSEN
Aandacht voor het beheren en optimaliseren van processen kan het risico van privacy-inbreuken en inefficiënties minimaliseren. Defensie werkt aan het effectief integreren van verbeterde processen met bestaande structuren en het bereiken van een adequaat volwassenheidsniveau van informatiehuishouding en compliance.

- **Begeleiding en ondersteuning**
  Bij de inrichting van processen en systemen t.b.v. de aansturing van de uitvoering kan aandacht voor privacyaspecten vroegtijdig worden geïntegreerd om inbreuken op rechten van betrokkenen te voorkomen. Grenzen aan en expliciteringen van bevoegdheden door beheer en de organisatie van processen rondom het geven en uitvoeren van opdrachten, kan helpen te voorkomen dat persoonsgegevens voor oneigenlijke doeleinden worden gebruikt. De Wodg en daaruit voortvloeiend beleid biedt de basis voor het aanvullen van bestaande compliance-processen, met specifieke verantwoordelijkheden voor commandanten en privacyfunctionarissen, zoals het bijhouden van een register met Wodg-verwerkingen. In de MvT wordt op dit punt opgemerkt dat hiertoe diverse onderdelen nauw dienen samen te werken, waarbij de operatie, IT, beleids- en privacy functies een belangrijke rol vervullen. Om deze taak uit te voeren dienen de betreffende organisatieonderdelen binnen de defensieorganisatie te worden versterkt.

- **Evaluatie en incidentmanagement**
  Door voortdurende evaluatie en rapportage wordt naleving van privacyregels versterkt, wat helpt bij het vermijden van ongewenst gebruik. Dit draagt bij aan het systematisch toetsen van militaire doctrines aan juridische kaders en interpretaties. Incidentmanagement en feedbackmechanismen helpen bij het detecteren en adresseren van onvoldoende afbakening van doelbinding en een (te) ruime toegang tot

persoonsgegevens en om de naleving van privacybeginselen te verbeteren.

- **Toezichthoudende processen**
  Wanneer sprake is van activiteiten en verwerkingen die een meer dan geringe inbreuk maken op rechten en vrijheden van betrokkenen is aanvullend toezicht noodzakelijk. De Autoriteit persoonsgegevens (AP) toetst de gegevensverwerkingen door de Minister van Defensie. De AP is op grond van de artikelen 6 lid 3 en 15 lid 1 UAVG verantwoordelijk voor zowel het externe toezicht op de naleving van de bepalingen uit de AVG en UAVG alsmede andere gegevensverwerkingen op grond van nationale wetgeving. De AP is daarmee ook verantwoordelijk voor het toezicht op de gegevensverwerkingen overeenkomstig dit wetsvoorstel. Daarnaast is op grond van artikel 39 lid 1 onder a, AVG de Functionaris Gegevensbescherming binnen Defensie verantwoordelijk voor het intern toezicht op zowel de van overeenkomstige toepassing verklaarde bepalingen uit de AVG en UAVG alsmede op de bijzondere regels die in hoofdstuk 4 van het wetsvoorstel worden gesteld. Voor bepaalde, meer vergaande bevoegdheden, wordt achteraf melding gedaan aan de AP (bijvoorbeeld artikel 4.12 lid 5).
  Daarnaast is in art. 4.17 opgenomen dat de Minister van Defensie de wijze waarop uitvoering wordt gegeven aan de taken, bevoegdheden en verplichtingen zoals bepaald in hoofdstuk 4 van het wetsvoorstel laat toetsen. De resultaten hiervan worden gerapporteerd aan de Staten-Generaal.

DATA
Door datamanagement op een hoger volwassenheidsniveau te brengen en door te zorgen voor naleving van bestaande regelgeving worden risico's zoals lage datakwaliteit en datalekken verminderd. Gezien de huidige datavolwassenheidsniveaus en systeembeperkingen zijn blijvende inspanningen nodig om dit effectief te implementeren.

- **Datamanagement en innovatie**
  Blijvend investeren in automatische datalabeling en hulpmiddelen voor versiebeheer verhoogt de betrouwbaarheid en vermindert fouten, wat de kans op identiteitsdiefstal en datalekken vermindert. Daarbij dient Defensie verzamelingen van persoonsgegevens te beperken tot wat strikt noodzakelijk is voor specifieke doeleinden, en vast te houden aan de oorspronkelijke doelstelling waarvoor persoonsgegevens zijn verzameld.

- **Tijdig verwijderen van gegevens**
  Om niet-beoogd hergebruik te voorkomen, dienen data-levenscycli zo te worden ingericht dat persoonsgegevens die vernietigd moeten worden, ook daadwerkelijk vernietigd worden. Ook dient te worden voorkomen dat onnodige informatie (te) lang wordt bewaard (bijv. antwoorden op de enquête). Door specifieke richtlijnen voor gegevensgebruik en -verzameling, bewaartermijnen en vernietigingsprocedures in het kader van de Wodg op te stellen en op de naleving hiervan toe te zien, zal Defensie ervoor zorgen dat data op een verantwoorde wijze wordt gebruikt. De Wodg bepaalt in artikel 4.3 de regels met betrekking tot de omgang met bewaartermijnen, waarbij het mogelijk is om bij AMvB nadere regels te stellen die niet-beoogd hergebruik dienen te voorkomen.

TECHNOLOGIE
Investeren in technologie helpt gegevensbescherming by-design te versterken en risico's voor betrokkenen effectief te minimaliseren.

- **Anonimiseren en pseudonimiseren**
  Het wetsvoorstel benadrukt het belang om persoonsgegevens te anonimiseren dan wel te pseudonimiseren. Een algemene waarborg is om persoonsgegevens die niet zijn verwijderd - rekening houdend met de stand van de techniek, de uitvoeringskosten, de aard, de omvang, de context van de verwerking, de risico's voor de rechten en vrijheden van natuurlijke personen en de risico's voor de gereedheid -, worden geanonimiseerd dan wel gepseudonimiseerd, tenzij het doel van de verwerking zich daartegen verzet. Anonimiseren en pseudonimiseren[62] zijn belangrijke maatregelen om persoonsgegevens te beveiligen (zie hierna).

- **Beveiliging**
  Implementatie van beveiligingsmaatregelen zoals encryptie, hashing en logging helpt om risico's van ongeautoriseerd gebruik te verminderen. Hiermee wordt de continuïteit, integriteit en vertrouwelijkheid van persoonsgegevens gewaarborgd. Hiervoor wordt ook verwezen naar het Defensie Beveiligingsbeleid.

- **Ethisch gebruik van technologieën**
  Door gebruik te maken van Privacy Enhancing Technologies (PET's) en het uitvoeren van audits op (technische) specificaties kunnen ethische risico's van technologiegebruik (bijvoorbeeld discriminatie door profilering) inzichtelijk worden gemaakt en de gegevensbescherming worden versterkt. Vanwege uitdagingen rondom de integratie met bestaande legacy-systemen en het capaciteitsniveau van IT-personeel, is hier expliciet aandacht voor nodig bij de aanschaf en implementatie van technologische hulpmiddelen.

Tabel: maatregelen gekoppeld aan risico's

Risico's (H16)	**Pijler**	**Maatregelen (H17)**
Verlies van controle over persoonsgegevens door onduidelijke taakafbakening tussen (overheids-)instanties	Strategie	• Codificatie van taken en verantwoordelijkheden • (Beleids)afspraken en richtlijnen voor gegevensverstrekkingen • Communicatie(plannen) en betrokkenheid
	Mensen	• Gedrag en bewustwording
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
Ongeautoriseerd gebruik van persoonsgegevens door gebrek aan regels (*scope creep*)	Strategie	• Besturing en verantwoordelijkheidstoewijzing • (Beleids)afspraken en gegevensverstrekking
	Mensen	• Gedrag en bewustwording
	Processen	• Begeleiding en ondersteuning • Evaluatie en incidentmanagement • Toezichthoudende processen
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Anonimiseren en pseudonimiseren • Beveiliging
Schade door inadequaat gegevensbeheer en	Mensen	• Gedrag en bewustwording
	Processen	• Begeleiding en ondersteuning • Evaluatie en incidentmanagement

[62] Voor de AVG zijn gepseudonimiseerde gegevens nog steeds persoonsgegevens, geanonimiseerde gegevens zijn dit niet.

gebrekkige beveiliging (inclusief incident management)		• Toezichthoudende processen
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Anonimiseren en pseudonimiseren • Beveiliging
Ongewenste profilering en discriminatie door geautomatiseerde systemen	Mensen	• Gedrag en bewustwording; datageletterdheid
	Processen	• Begeleiding en ondersteuning
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Ethisch gebruik, inzet van *Privacy Enhancing Technologies* (PET's), uitvoeren van audits • Anonimiseren en pseudonimiseren
Beperkte mogelijkheid tot uitoefening van rechten en toegang tot juridische bescherming door gebrek aan transparantie	Strategie	• Besturing en verantwoordelijkheidstoewijzing • (Beleids)afspraken en gegevensverstrekking
	Processen	• Begeleiding en ondersteuning
Verandering van gedrag door monitoring (*chilling effect*)	Strategie	• Communicatie(plannen) en betrokkenheid
	Mensen	• Gedrag en bewustwording
Te ruime verwerking van persoonsgegevens in het kader van de enquête	Strategie	• Besturing en verantwoordelijkheidstoewijzing • Beleidsafspraken en richtlijnen • Communicatie en betrokkenheid
	Mensen	• Gedrag en bewustwording
	Processen	• Begeleiding en ondersteuning • Evaluatie en incidentmanagement
	Data	• Datamanagement en innovatie • Tijdig verwijderen van gegevens
	Technologie	• Anonimiseren en pseudonomiseren • Beveiliging

Ondertekening

Om de DPIA formeel vast te stellen, is het noodzakelijk deze te ondertekenen, zodat het duidelijk is dat de DPIA door de verantwoordelijke(n) akkoord is bevonden.

Naam verantwoordelijke(n)	
Directie/afdeling verantwoordelijke(n)	
Functie verantwoordelijke(n)	
Datum ondertekening	
Handtekening	