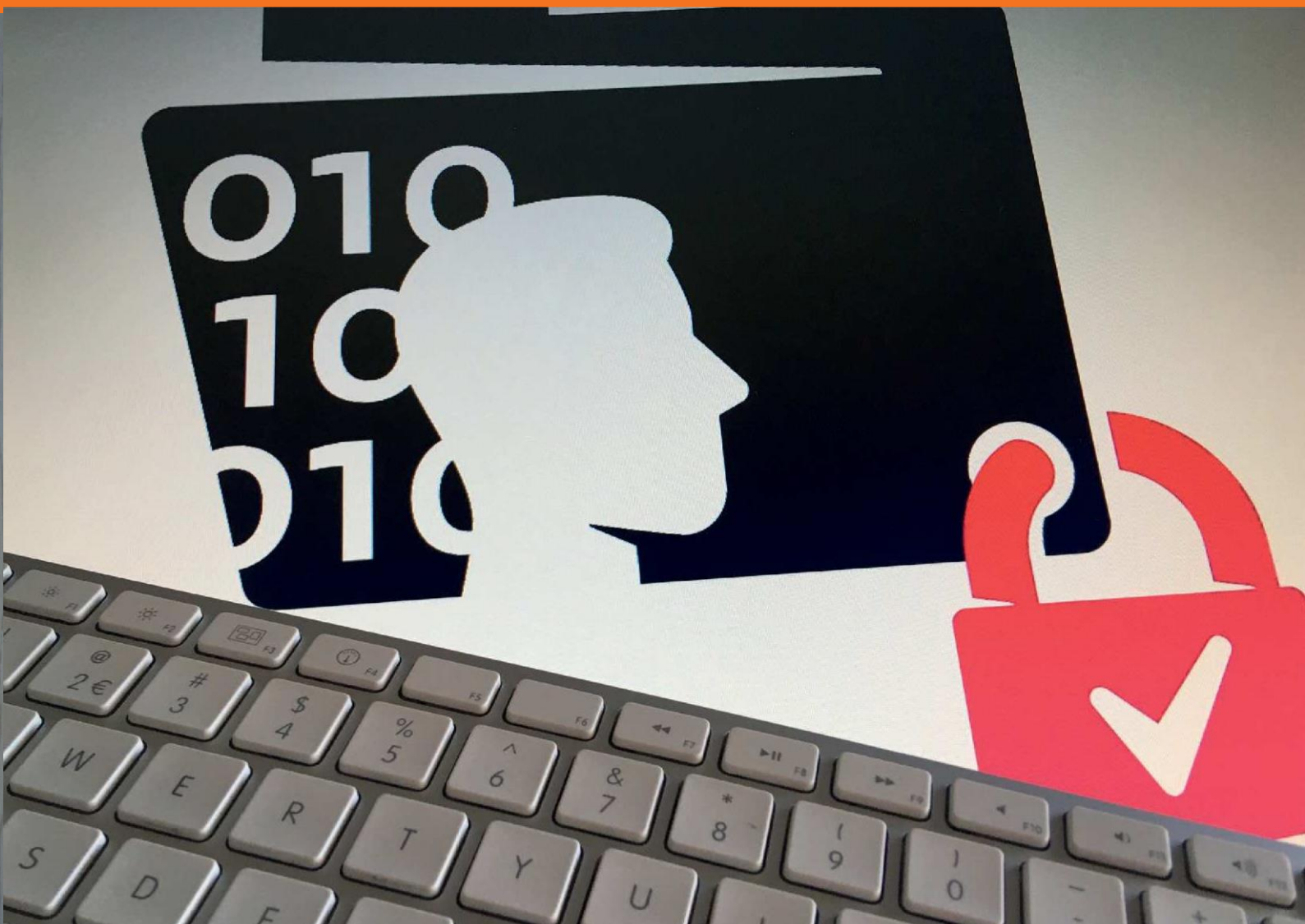
Ministerie van Defensie

Toezichtjaarverslag 2020

Functionaris voor de Gegevensbescherming



Colofon

Kalvermarkt 32
Postbus 20701
2511 CB Den Haag
Bezoekadres: Plein Kalvermarkt

Vindplaats

Het Toezichtjaarverslag FG 2020 is te vinden op de intranetsite van de toezichthouders:
http://intranet.mindef.nl/bs/bedrijfsvoering/processen/Toezicht/Toezichtjaarplannen.aspx

Inhoud

Inleiding

De Functionaris voor Gegevensbescherming (FG) is binnen het Ministerie van Defensie belast met het houden van toezicht op de naleving van de Algemene verordening gegevensbescherming (Avg) en de Wet politiegegevens (Wpg).

De Avg (Verordening EU 2016/679) reguleert de algemene verwerking van persoonsgegevens, gebaseerd op privaatrechtelijke en bestuurlijke rechtsverhoudingen. De Avg is een Europese Verordening die rechtstreekse werking heeft in de lidstaten. De Avg heeft op 25 mei 2018 de Wet bescherming persoonsgegevens vervangen. De inwerkingtreding van de Avg, nu bijna 3 jaar geleden, was met recht een mijlpaal voor het gegevensbeschermingsrecht en gaf een nieuwe impuls aan het privacybegrip. De Avg raakt bij het Ministerie van Defensie hoofdzakelijk aan de verwerking van persoonsgegevens binnen de diverse bedrijfsvoeringsprocessen. Gaat Defensie op juiste wijze om met persoonlijke gegevens van militairen en burgermedewerkers, bijvoorbeeld bij het toepassen van nieuwe technologieën op het terrein van personeelszorg? Maar de Avg is ook van toepassing op persoonsgegevens van derden van buiten Defensie die betrokken worden in civiele of bestuursrechtelijke aangelegenheden. Zoals partijen die in een juridische procedure zijn verwikkeld met Defensie. En zo valt bijvoorbeeld ook de verwerking van persoonsgegevens van reizigers en vreemdelingen door de Koninklijke Marechaussee op grond van de Vreemdelingenwet onder de werkingssfeer van de Avg.

De verwerking van persoonsgegevens door de bevoegde autoriteiten op het terrein van politie en justitie vallen buiten de materiële werkingssfeer van de Avg. Het Europees parlement en de Raad van de Europese Unie hebben hiervoor een aparte, naast de Avg staande, richtlijn gegevensbescherming opsporing en vervolging aangenomen (Richtlijn EU 2016/680). De verwerking van persoonsgegevens in verband met opsporing en vervolging, zoals de uitvoering van de politietaken door de Koninklijke Marechaussee, dient conform deze Europese richtlijn plaats te vinden. De richtlijn heeft, in tegenstelling tot de Avg, geen rechtstreekse werking. De richtlijn is in Nederland met ingang van 1 januari 2019 geïmplementeerd door aanpassing van de bestaande Wpg en de Wet justitiële en strafvorderlijke gegevens. Waar dit voorheen slechts facultatief was voorgeschreven in de Wet is de Minister van Defensie inmiddels als overheidsorgaan én als bevoegde autoriteit op het terrein van politie en justitietaken wettelijk verplicht een FG aan te stellen. Vanaf 2019 is binnen de defensieorganisatie voorzien in aanstelling van een (additionele) FG voor de Wpg. Het toezicht op de naleving van de Wpg is vanaf 2020 structureel opgenomen in het Toezichtjaarverslag FG.

Voor u ligt het verslag van de werkzaamheden en bevindingen in het jaar 2020 van de beide FG's. Dit verslag vindt zijn grondslag in artikel 38 lid 3 van de Avg en artikel 1.5, lid 3 van de Regeling Avg Defensie (Besluit 15 mei 2018, Staatscourant 2018, nr. 28291) en in artikel 36 lid 4 Wpg en artikel 1.6 lid 3 van de regeling Wpg Defensie (Besluit 16 december 2018, Staatscourant 2018, nr. 72552, laatstelijk gewijzigd bij besluit van 8 november 2019 Staatscourant 2019, nr. 62419) .

Hierin is bepaald, dat de FG's jaarlijks hun bevindingen rapporteren over de naleving van de Avg, de Uitvoeringswet Avg en de Wpg binnen het Ministerie van Defensie.

In de SG-Aanwijzing 948 "Toezicht bij Defensie" is voorgeschreven, dat de FG jaarlijks, uiterlijk op 15 maart een verslag opstelt.

Met dit jaarverslag wordt invulling gegeven aan bovengenoemde rapportageverplichtingen over het jaar 2020.

De Functionaris voor Gegevensbescherming Algemene verordening gegevensbescherming

mevr. mr. O.L. Stenhuis-Kok

De Functionaris voor Gegevensbescherming Wet politiegegevens

mr. K.M.M. Weijers

1. Belangrijkste bevindingen FG

Het jaar 2020 stond voor de Avg, evenals voorgaande jaren, vooral in het teken van het verder bestendigen van de sinds 25 mei 2018 in werking getreden Avg. Voor de Wpg geldt dat sinds 1 januari 2019 belangrijke wijzigingen in de Wet politiegegevens zijn doorgevoerd ter implementatie van de richtlijn EU 2016/680.

De FG signaleert dat de structurele inbedding van privacygovernance en risicomanagement bij Defensie nog volop in ontwikkeling is. Defensie heeft een aantal maatregelen getroffen die bijdragen aan de beheersing van de privacyrisico's ten einde de naleving van de Avg en Wpg te borgen. De taken, verantwoordelijkheden en rapportagelijnen rond Avg en Wpg zijn vastgelegd en grotendeels ingericht conform het beleid. Ook de Avg-organisatie is grotendeels ingevuld en er is een register van verwerkingsactiviteiten gerealiseerd om inzicht te geven in welke verwerkingen van persoonsgegevens er binnen Defensie plaatsvinden.

Door beleidsinitiatieven, technologische ontwikkelingen en een toenemend privacybewustzijn nemen kansen voor privacy en risico's op privacyschendingen toe. Privacy is niet alleen een last maar ook een lust: een grondrecht om na te leven juist in het digitale tijdperk. Voldoende capaciteit en middelen om daarmee de Avg/Wpg functie te professionaliseren zijn daarbij essentieel.

Meer aandacht is nodig voor systematische borging van Avg en Wpg -compliancy binnen de defensieorganisatie, waarbij aandacht wordt gevraagd voor voldoende capaciteit en middelen, inbedding in het reguliere risicomanagement en verhoging van de kwaliteit van registraties in het register van verwerkingsactiviteiten.

Professionalisering van de Avg/Wpg functie is daarbij van belang. Om te beginnen door invulling te geven aan de recent door de Tweede Kamer aangenomen motie (Kamerstukken nr. 967925) rondom aanstelling van een CPO (een Chief Privacy Officer)[1].

Voor wat betreft gegevensbescherming ziet de top drie actiepunten (tevens aanbevelingen) er als volgt uit:

Aanbeveling 1:
Voorzie in voldoende capaciteit en middelen ter professionalisering van de Avg/Wpg functie en investeer op deze wijze in het vergroten van het kennisniveau van de Avg/Wpg.
Aanbeveling 2:
Besteed meer aandacht voor de beveiliging van persoonsgegevens bij de uitwisseling ervan met externe partijen en investeer in het verhogen van de bewustwording (inkoopketen).
Aanbeveling 3:
Completeer en documenteer het Defensie verwerkingenregister (inclusief DPIA's en verwerkersovereenkomsten) en bevorder het bijhouden van een geactualiseerd overzicht van geregistreerde datalekken (inbreuken op de beveiliging).

[1] zie: (https://www.tweedekamer.nl/kamerstukken/detail?id=2021Z02217&did=2021D04899)

2. Algemeen

Tijdens de cyber operations conferentie ("CODE 2020") in München op 10 november 2020 wees de minister op het belang van de doorontwikkeling van de informatiegestuurde krijgsmacht en het verbeteren van de Europese digitale weerbaarheid en soevereiniteit [2].

" Informatie als wapen, dát is het nieuwe slagveld. Wie snel informatie kan filteren, verwerken, analyseren en doorgeven aan de mensen in het slagveld, die wint de strijd."

"Onze Defensieorganisaties verwerken cruciale informatie over zaken van leven of dood, die gemakkelijk kan worden gemanipuleerd door nieuwe technologieën. Het is informatie die we moeten beschermen, om de beschikbaarheid en integriteit te behouden."

Met de aandacht voor de verbetering van onze weerbaarheid tegen digitale dreiging en de doorontwikkeling naar een informatiegestuurde krijgsmacht werd hierna terecht het verband gelegd met onze Europese grondrechten, waaronder zeker ook de Algemene verordening gegevensbescherming (Avg).

"Als we als EU het digitale domein willen besturen, moeten we dat doen op basis van onze Europese waarden voor vrijheid, democratie en mensenrechten. Alleen dan kunnen we 'whole of society' approach bereiken."

Dit brengt nieuwe inzichten en wij realiseren ons hierdoor dat waar voorheen de nadruk van de Avg vooral lag op bedrijfsvoeringsprocessen, de Avg ook een belangrijkere factor vormt bij de inzet en militaire operaties.

Met de inwerkingtreding van de Avg in mei 2018 is binnen de gehele Europese Unie uniforme wetgeving ontstaan voor adequate omgang met persoonsgegevens die een hoog privacybeschermingsniveau voor de burgers biedt. Een zelfde geharmoniseerde basis is neergelegd in de Europese richtlijn voor de verwerking van persoonsgegevens voor politie- en justitietaken (EU 2016/680), in Nederland omgezet in de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg).

Het Ministerie van Defensie geeft actief invulling aan de bescherming van de privacy van burgers inclusief haar eigen medewerkers door effectief beleid te voeren en te zorgen voor goede implementatie en naleving van deze wetgeving. De Functionaris voor Gegevensbescherming (FG) speelt hierbij zowel een voorlichtende, een adviserende als een toezichthoudende rol, daarbij gesteund door Avg-coördinatoren en privacyfunctionarissen van de verschillende defensieonderdelen. De eind 2020 gepresenteerde Defensievisie 2035 benadrukt andermaal dat Defensie ernaar streeft zich verder te ontwikkelen als slimme, technologisch hoogwaardige en informatie gestuurde krijgsmacht. En door toenemende digitale en hybride dreigingen vormen de informatie-omgeving en

[2] https://www.defensie.nl/actueel/nieuws/2020/11/10/europa-moet-ook-digitaal-van-zich-kunnen-afbijten

de verwerking van persoonsgegevens belangrijke componenten van het strijdtoneel.

De Avg en de Wpg geven, naast regels over het vastleggen en gebruiken van persoonsgegevens, ook regels over het toezicht op de naleving. De Autoriteit persoonsgegevens (Ap) is in de Uitvoeringswet Algemene verordening gegevensbescherming aangewezen als de nationale toezichthouder. De Ap kan in bepaalde gevallen bestuurlijke boetes opleggen of bestuursdwang (dwangsom) toepassen. Bijvoorbeeld voor het niet (goed) naleven van de meldplicht met betrekking tot datalekken, kan de Ap een hoge boete (tot max. 20.000.000,- Euro) opleggen. Binnen het domein van de Wpg heeft de Ap een overeenkomstige rol en positie als nationale externe toezichthouder.

De Avg biedt de mogelijkheid om, naast de externe toezichthouder (de Ap), een interne toezichthouder, te weten een Functionaris voor Gegevensbescherming (FG), te benoemen. Overheidsorganisaties zijn op grond van zowel de Avg als de Wpg verplicht een FG aan te stellen. Het aanstellen van een FG doet overigens geen afbreuk aan het toezicht en de bevoegdheden van de Ap. De autoriteit hanteert in de praktijk wel de lijn, dat zij zich terughoudend opstelt als een FG is benoemd.

De wettelijke taken van een FG zijn: het houden van toezicht en het toezien op de afwikkeling van klachten en het evalueren van incidenten ter zake van het verwerken van persoonsgegevens binnen het Ministerie van Defensie. Het toezicht betreft vooral rechtmatigheidstoezicht en ziet op de naleving van het bij of krachtens de Avg, de UAvg en de Wpg bepaalde.

De taken en werkzaamheden van de FG Defensie zijn nader omschreven in artikel 1.5, tweede lid, van de Regeling Avg Defensie (Staatscourant 2018, nr. 28291) en artikel 1.6 van de Regeling Wpg Defensie (Staatscourant 2018, nr. 7552, laatstelijk gewijzigd 01 januari 2020, Staatscourant 2019, nr. 62419).

De FG bij Defensie houdt geen toezicht op de verwerking van persoonsgegevens die vallen onder de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv). Toezicht en controle daarop geschiedt door de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten.

3. Trends / meerjaren-beleid in het privacydomein

Op basis van de toezichtresultaten 2014-2020 ('meerjarenbeeld') kunnen de volgende trends binnen het privacydomein worden vastgesteld. De vermelde trends worden hierna nader toegelicht:

1. Privacybewustzijn neemt toe binnen de defensieonderdelen.

2. Privacy wordt steeds meer als een multidisciplinair onderwerp gezien.

3.1 Privacybewustwording

De afgelopen jaren

Door de jaren heen is door de defensieorganisatie veel werk gemaakt van privacybewustwording. Daar waar aanvankelijk nog volstaan kon worden met het doen van een melding van een verwerking aan de FG is vanaf 2013 een Privacy Impact Assessment (PIA) verplicht bij de ontwikkeling van nieuwe wetgeving/beleid waarmee de bouw van nieuwe ict-systemen of de aanleg van grote databestanden wordt voorzien. Een PIA fungeert hierbij als hulpmiddel om privacyrisico's voor betrokkenen op gestructureerde en heldere wijze in kaart te brengen. Het model PIA is in 2017 geëvalueerd en vervolgens is het nieuwe model in 2017 voor de rijksdienst vastgesteld door de Ministerraad. Ook een onderwerp als de meldplicht voor datalekken (vanaf 2016) heeft voor een groeiende bewustwording gezorgd rondom het thema privacy.

Algemene verordening gegevensbescherming (Avg)

Het jaar 2020 heeft evenals 2019 op het gebied van het gegevensbescherming en privacy vooral in het teken gestaan van compliance en control en het waar nodig verder implementeren van de sinds 25 mei 2018 in werking getreden Avg. Op hoofdlijnen heeft de defensieorganisatie goede stappen gemaakt, nu is vooral aandacht nodig voor het verder bestendigen van de beleidsmatig, technisch en organisatorisch ingerichte compliance en control maatregelen en het inventariseren van de specifieke en uitzonderlijke verwerkingsactiviteiten, zodat Defensie ook voor die buitengewone verwerkingen compliant en in control kan komen. Dit betreft een aantal buitengewone verwerkingsactiviteiten, bijvoorbeeld waarbij bijzondere of gevoelige persoonsgegevens worden verwerkt, zoals biometrische en genetische gegevens en de uitwisseling en doorgifte van persoonsgegevens in internationaal verband bijvoorbeeld binnen bondgenootschappelijke samenwerkingsverbanden en internationale organisaties.

Alle defensieonderdelen hebben de afgelopen jaren bewustwordingsacties uitgevoerd. Dit betreft bijvoorbeeld het geven van presentaties bij de eenheden, het opstellen van intranetpagina's met

informatie over de Avg, nieuwsbrieven en bijzondere aandacht voor de privacy bij de introductie van

nieuwe defensiemedewerkers en gedurende de coronapandemie. Door beleidsinitiatieven, technologische ontwikkelingen en een toenemend privacybewustzijn nemen kansen voor privacy en risico's op privacyschendingen toe. Privacy is niet alleen een last maar ook een lust: een grondrecht om na te leven juist in het digitale tijdperk. Een (meerjarig) bewustwordingsprogramma kan daarbij een rol spelen om te zorgen voor een meer systematische borging van Avg en Wpg-compliance binnen de defensieorganisatie.

Privacy in het algemeen en datalekken in het bijzonder konden daarmee in 2020 rekenen op de nodige aandacht in de politiek en de media. Vanaf het begin van de coronapandemie is de defensiemedewerker, vaak genoodzaakt tot veel thuiswerken voor zover mogelijk, met regelmaat geïnformeerd door middel van nieuwsberichten over de risico's (bijv. videobellen), die dat met zich meebrengt.

Het op peil houden en verdiepen van de privacybewustwording binnen Defensie vraagt ook de komende jaren veel inspanning van de Avg en Wpg organisatie (beheerders, coördinatoren, privacyfunctionarissen en FG's).

3.2 Trends en ontwikkelingen

Van juridisch naar multidisciplinair vraagstuk

De afgelopen jaren werd de Wet bescherming persoonsgegevens (Wbp; voorloper Avg), vooral gezien als een juridisch georiënteerd vraagstuk. De IT-ontwikkelingen hebben dit beeld echter achterhaald. Het gebruik van (steeds meer) informatie- en communicatietechnologieën heeft voor een groot deel onze hedendaagse maatschappij bepaald. Het gaat daarbij niet zozeer om de technologie op zichzelf, maar meer om de groeiende hoeveelheid toepassingsmogelijkheden (internet, gegevenspakhuizen, datamining, big data etc.), die gepaard gaan met een groeiend beslag op persoonsgegevens en de koppelingen die daarmee te maken zijn.

Privacy als multidisciplinair vraagstuk

Door de snelheid en de complexiteit van de technologische ontwikkelingen van de afgelopen jaren zijn de gevolgen voor betrokkenen lastig te overzien. Doordat de ontwikkelingen elkaar steeds sneller opvolgen is het van belang om de balans tussen technologie en privacy goed in het oog te houden. De Avg is in deze tijd niet meer te zien als een uitsluitend juridisch onderwerp. Het raakt tal van domeinen (IT/inkoop/beveiliging/integriteit/archivering) en is om die reden dan ook complex geworden.

Juist ook in samenwerkingsrelaties met (civiele) partners is privacy by design and default het devies.
Sinds einde 2013 is het opstellen van een zogenaamde Privacy Impact assessment (kortweg: PIA of DPIA wat staat voor Data Protection Impact Assessment) verplicht alvorens er wordt gestart met een verwerking van persoonsgegevens waar veel of bijzondere persoonsgegevens bij worden verwerkt. Door een DPIA uit te voeren wordt de impact op de privacy zichtbaar gemaakt voor betrokkenen (degenen wiens persoonsgegevens worden verwerkt).

Ook te treffen beveiligingsmaatregelen worden beschreven in een DPIA. In geval van verwerkingen van persoonsgegevens waarbij een verwerker wordt ingeschakeld, dient tevens een verwerkersovereenkomst te worden afgesloten. De afgelopen jaren is gebleken, dat de

beveiliging bij gegevensuitwisseling met derde partijen niet altijd op orde is en daarom aandacht verdient.

Risico's bestaan er vooral binnen andere sectoren waarin Defensie samenwerkt met civiele partners (onderzoeken, werving en selectie), dan wel waar onderlinge gegevensverstrekking/uitwisseling plaatsvindt (zorginstellingen, UWV, ABP, Douane, OM). Niet voor niets zijn deze verwerkingen door de FG de afgelopen jaren aangemerkt als toezichtspeerpunt.

Toekomstige technologische ontwikkelingen in samenhang met privacy vraagstukken

De Defensievisie 2035 Vechten voor een veilige toekomst onderbouwt het belang van informatiegestuurd organiseren in optreden en onderstreept dat Defensie ook toegerust moet zijn om binnen de geldende ethische en juridische kaders, op te treden in de informatieomgeving. In lijn met deze visie is het groeiend belang van gegevensbescherming, informatievoorziening en informatiebeveiliging. Dit vereist eveneens een groei van de benodigde middelen voor gegevensbescherming die hieruit voortvloeien.

Naast de (D)PIA en de verwerkersovereenkomst is aandacht voor beveiligings- en organisatorische maatregelen essentieel om de privacy van betrokkenen te borgen. Door maatregelen als encryptie, autorisatiematrixen en logging kan ook een balans worden gevonden tussen de technologische ontwikkelingen van vandaag de dag en het waarborgen van de privacy van betrokkenen.

Binnen en naast de regulier uit te voeren toezichtwerkzaamheden zal aansluiting worden gezocht bij de focusgebieden van de Ap te weten: datahandel, digitale overheid en artificiële intelligentie en algoritmes, die voor de periode 2020 tot en met 2023 zijn aangewezen in het visiedocument 'Dataprotectie in een digitale samenleving'. Behalve voor de privacy en het gegevensbeschermingsrecht brengen deze ontwikkelingen ook menselijke en ethische implicaties met zich mee.

Binnen Defensie is de opkomst zichtbaar van technologische toepassingen voor biometrische herkenning, verwerking van genetische gegevens en het monitoren van prestaties en gezondheidsaspecten. Met de COVID-19 pandemie zijn daar in 2020 ook vele vraagstukken rond het monitoren van gezondheid en het uitvoeren van medische metingen en testen bijgekomen. De komende jaren is van belang om deze specifieke en uitzonderlijke verwerkingsactiviteiten te inventariseren, opdat Defensie ook voor die buitengewone verwerkingen compliant kan worden en in control kan komen. Professionalisering van de Avg/Wpg functie is daarvoor noodzakelijk.

Tot slot spelen er op internationaal terrein diverse vraagstukken op het gebied van gegevensbescherming, zoals de uitwisseling en doorgifte van persoonsgegevens in internationaal verband bijvoorbeeld binnen bondgenootschappelijke samenwerkingsverbanden en internationale organisaties.

4. Normering en beoordeling Avg en Wpg

In het Toezichtberaad Defensie, het samenwerkingsverband van de interne toezichthouders van Defensie) is het onderwerp normering herhaaldelijk aan de orde gekomen. Hierbij werd door de voorzitter aangegeven, dat beoogd wordt dat de toezichthouders in hun jaarplannen en jaarverslagen rapporteren op basis van een vastgestelde normering. Hierdoor ontstaat een duidelijk beeld, een soort *stand van zaken* van, of een *thermometer* voor de situatie bij Defensie.
Hieronder wordt ingegaan op de naleving van deze normen door de Avg- en Wpg (onder)beheerders in 2020.

4.1 De Avg-coördinator en Wpg-privacyfunctionaris

Op grond van artikel 1.3, lid 3, van de Avg Regeling wijst een Avg-(onder)beheerder binnen zijn dienstonderdeel een Avg-coördinator aan, die de uitvoering van de wet en de feitelijke handelingen die daarvoor nodig zijn, binnen zijn dienstonderdeel coördineert. Hij doet hiervan mededeling aan de FG. De Avg-coördinatoren hebben een cruciale rol bij de implementatie en naleving van de Avg bij Defensie. Op grond van artikel 34 van de Wpg en artikel 1.4 van de Regeling Wpg Defensie dient CKmar als Wpg-beheerder één of meerdere privacyfunctionarissen aan te wijzen.

Voor 2020 zijn de volgende aspecten door de FG ter beoordeling bezien.

a Is er onder de verantwoordelijkheid van de Avg-(onder)beheerder een Avg-coördinator of Wpg-privacyfunctionaris aangewezen?
b Is deze Avg-coördinator of Wpg-privacyfunctionaris formeel aangemeld bij de FG?
c Was deze Avg-coördinator of Wpg-privacyfunctionaris door de Avg-(onder)beheerder bekend gesteld in de organisatie?
d Heeft deze Avg-coördinator of Wpg-privacyfunctionaris de juiste opleiding/training gekregen voor de functie?
e Krijgt de Avg-coördinator of Wpg-privacyfunctionaris de benodigde geformaliseerde tijd, middelen en ruimte om de taak naar behoren te kunnen uitvoeren?
f Is de taak van Avg-coördinator of Wpg-privacyfunctionaris opgenomen in zijn functieomschrijving?

	CZSK	CLAS	CLSK	KMar AVG	KMar Wpg	BS (apparaat)	BS DOPS v	BS (defensie breed)	DMO	DMO / JIVC	DOSCO
a	ii	i/ii	ii	ii			v			ii	ii
b											
c											
d											
e					iii						
f				iv							

Ja/goed	
Onvoldoende	
Nee	
Onbekend / geen info	

Bevindingen:

i. M.i.v. 1 oktober 2019 is de Avg-coördinator aangesteld en het Avg onderbeheerderschap belegd bij de brigades. In 2020 was slechts 1 (onder)Avg coördinator werkzaam.

ii. De rol van Avg-coördinator was bij de meeste defensieonderdelen tot 2019 belegd als neventaak en (nog) niet opgenomen in de taakomschrijving. Daardoor kwamen veel Avg coördinatoren, vaak door gebrek aan tijd/andere prioritering van taken, niet (voldoende) toe aan hun Avg taak. Capaciteitsuitbreiding binnen de BS is voor een deel nu niet ingevuld en voor een deel (tijdelijk) per einde 2020. Van belang is nu de structurele borging. Een aantal defensieonderdelen (CZSK, KMar, CLAS, DOSCO,CLSK) heeft in de loop van 2019 de Avg-coördinator functie (her)ingericht. De privacy ontwikkelingen vragen immers om een op privacygebied vaardige Avg-coördinator, alsmede een goed opgeleid en geëquipeerd netwerk van Avg-functionarissen die multidisciplinair inzetbaar zijn om aan hun taak te kunnen voldoen gelet op het door defensie gestelde ambitieniveau 'voldoende voor privacy; goed voor beveiliging'.

iii. Bij de KMar is ten aanzien van de Wpg verwerkingen de aanwijzing van een Wpg-coördinator verplicht. De Wpg hanteert de term 'privacyfunctionaris'. Binnen de KMar zijn formatief 2 VTE, Stafadviseur bij het Cluster Juridische Zaken hoofdzakelijk belast met de vervulling van de privacyfunctionaristaak en daarnaast belast met andere (aan gegevensbeschermingsrecht gerelateerde) juridische vraagstukken. Een groot deel van 2020 was slechts één van de twee Stafadviseursfuncties volledig beschikbaar, daarbij vanaf mei 2020 ondersteund door een tijdelijke aangestelde WPG-coördinator. De cursus Wpg-privacyfunctionaris aan de Politieacademie is al een aantal jaren niet meer gehouden, gezien de geringe vraag is er ook geen adequaat alternatief bij particuliere opleidingsinstellingen.

iv. 1 vte AVG-coördinator is te weinig capaciteit om alle taken en werkzaamheden uit te voeren. Het grote aantal verwerkingen, zowel in de bedrijfsvoering als in de operaties van e KMar en de werkdruk vanuit (innovatieve) projecten, audits en ketensamenwerking vergen meer capaciteit. De huidige functie van Avg-coördinator KMar eindigt in juni 2021. Er is nog niet besloten in welke vorm de functie wordt voortgezet.

v. DOPS heeft geen eigenstandige Avg-coördinator aangesteld; wel een interim functionaris. De functie is een vacature en de Stafofficier Integratie (SI) neemt deze taak tijdelijk waar. De SI is sinds mei 2020 werkzaam bij de DOPS en heeft geen Avg opleiding gehad. De vulling van de functie is belangrijk voor de continuïteit en kwaliteit van de coördinatie AVG/RGMO en daarmee aansluiting vanuit de operatie.

Aanbeveling:
Meer aandacht voor professionalisering van de Avg/Wpg functie en investeer op deze wijze in het vergroten van capaciteit en kennisniveau, zowel kwantitatief en kwalitatief waar noodzakelijk.

4.2 Jaarrapportage

Iedere Avg-beheerder behoort jaarlijks, vóór 1 januari, aan de FG te rapporteren over de naleving binnen zijn defensieonderdeel.

Voor het jaar 2020 is het volgende beoordeeld:
a. Heeft de Avg/Wpg-(onder)beheerder een jaarrapportage aan de FG aangeboden?
b. Is deze rapportage voor 1 januari aan de FG aangeboden?

	CZSK	**CLAS**	**CLSK**	**KMar Avg**	**KMar Wpg**	**BS (apparaat)**	**BS DOPS**	**BS (defensiebreed)**	**DMO / JIVC**	**DOSCO**
a										
b		i		i	i	i	i	ii	i	

Ja	
Nee	

Bevindingen:
i. Uitstel verzocht en begin 2021 de jaarrapportage ontvangen.
ii. Jaarrapportage ontvangen na 15/03/2021

4.3 DPIA/Gegevensbescherming Effectbeoordeling

Op grond van artikel 35 Avg en artikel 4c Wpg dient er wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen, voorafgaand aan de verwerking een beoordeling te worden uitgevoerd van de effecten van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

In artikel 3 van de Regeling Avg Defensie en artikel 3 van de Regeling Wpg Defensie is voorgeschreven dat de DPIA dient te worden uitgevoerd door de proceseigenaar als het om een bepaald uitvoerend proces of ict systeem gaat en door de betrokken beleidsdirectie voor zover het om een DPIA op wetgeving of beleid gaat. De Avg-coördinator vervult hierin een adviesrol, indien noodzakelijk kan hierbij aanvullende consultatie van de FG plaatsvinden. Na het doorlopen van de DPIA wordt het advies (appreciatie) ingewonnen van de FG. En dient te worden bepaald of er dusdanig hoge restrisico's zijn dat de verwerking middels de procedure van voorafgaande raadpleging dient te worden voorgelegd aan de Autoriteit persoonsgegevens. De proceseigenaar, doorgaans het betreffende defensieonderdeel of de verantwoordelijke beleidsdirectie, stelt uiteindelijk de definitieve DPIA vast. De DPIA dient te worden bijgevoegd in het register van verwerkingsactiviteiten. Vanaf 2017 wordt binnen de rijksoverheid gewerkt met een door de Ministerraad vastgesteld model DPIA. Dit model is leidend voor het uitvoeren van een DPIA voor verwerkingen van persoonsgegevens binnen de rijksdienst. Het doel van dit model is om, conform de eisen van de Europese privacyregels en de aanbevelingen uit het evaluatierapport, de bescherming van persoonsgegevens op een gestructureerde manier onderdeel te laten zijn van de belangenafweging en besluitvorming over voorgenomen gegevensverwerkingen binnen de rijksdienst. Vanaf de inwerkingtreding van de Avg dient een (definitieve) DPIA, voorafgaand aan de verwerking, te worden voorgelegd aan de FG voor advies. In 2020 zijn in totaal 18 DPIA's aan de FG voorgelegd ter appreciatie. Eind 2020 werden er in totaal ook 18 KMar DPIA's ter consultatie voorgelegd aan de FG. Na de consultatie volgt een revisie door de KMar waarna de DPIA's ter definitieve appreciatie aan de FG worden aangeboden. Eind 2020 waren er nog geen KMar DPIA's ter definitieve appreciatie voorgelegd.

Op grond van de Wpg geldt ook de verplichting tot het uitvoeren van DPIA's, hiervoor dient een aangepaste versie van het rijksmodel gehanteerd te worden. De KMar rapporteert dat er een omvangrijk aantal DPIA's zal moeten worden uitgevoerd op zowel bestaande als nog te starten verwerkingen. In 2020 zijn tientallen DPIA's gestart. Hiervoor is tijdelijk extra capaciteit vrijgemaakt of ingehuurd. Eind 2020 zijn 6 Wpg DPIA's ter consultatie voorgelegd aan de FG en werden nog geen Wpg DPIA's ter definitieve appreciatie voorgelegd.

Voor 2020 is de DPIA verplichting op de volgende aspecten door de FG ter beoordeling bezien:

a. Worden de wettelijke voorvragen juist doorlopen en wordt er een juiste interpretatie gegeven aan de DPIA verplichting?
b. Is er een goed overzicht van DPIA's die moeten worden uitgevoerd (incl. prioritering)?
c. Is de werkvoorraad in verhouding tot capaciteit (kwantitatief en kwalitatief) van de DPIA-teams
d. Wordt het Rijksformat juist gebruikt en volledig ingevuld:
   - is het proces voldoende beschreven?

- zijn wettelijke grondslagen en juridisch kader voldoende uitgewerkt?
- zijn risico's voldoende in kaart gebracht?
- zijn er afdoende mitigerende maatregelen genomen of bewuste restrisico's geaccepteerd door procesverantwoordelijke?
- is er sprake van formele vaststelling van de definitieve DPIA door verwerkingsverantwoordelijke?

e. Is de voorgeschreven interne procedure voor aanbieding ter advies van de DPIA juist doorlopen?
(consultatie/appreciatie FG en evt. voorafgaande raadpleging Ap)

f. Worden de vastgestelde DPIA's toegevoegd aan het register van verwerkingsactiviteiten?

	CZSK	CLAS	CLSK	KMar AVG	KMar Wpg	BS (apparaat)	BS DOPS ii	BS (defensiebreed)	DMO	DMO/ JIVC	DOSCO
a							ii				
b											
c				i	i						
d											
e											
f					iv						

Ja/goed	
Onvoldoende	
Nee	
Onbekend / geen info	
Niet van toepassing	

Bevindingen:

i. De benodigde capaciteit voor het invullen van de DPIA verplichtingen bij de KMar werd in 2020 voldoende ingericht door inhuur en tijdelijke capaciteit. Er was sprake van een werkachterstand, kwantitatief en kwalitatief, die is deels ingehaald. Omdat continuïteit van de inhuur en tijdelijke capaciteit in 2021 onzeker is wordt dit punt als onvoldoende beoordeeld.

ii. Op de verwerkingen vanuit BS/DOPS waarop de regeling gegevensverwerking militaire operaties van toepassing is, geldt geen DPIA verplichting.

iii. zie ook 4.4 De KMar is per 1 januari 2019 op grond van haar wettelijke verplichting gestart met inventariseren en registreren van de Wpg verwerkingen. Aangezien het Avg-verwerkingenregister van Defensie op dat moment nog niet aangepast en geschikt gemaakt was voor het registreren van Wpg verwerkingen is hiervoor een tijdelijke voorziening getroffen. Het voornemen is om het AVG verwerkingenregister vanaf 2021 te gaan vullen en ook alle Wpg verwerkingsactiviteiten hierin te registreren en de tijdelijke voorziening daarna op te heffen.

Aanbeveling:

Meer aandacht voor professionalisering van de Avg/Wpg-functie en investeer in capaciteit en in het vergroten van het kennisniveau op het gegevensbeschermingsdomein.

Completeer en documenteer het Defensie verwerkingenregister (incl. DPIA's en verwerkersovereenkomsten) en bevorder het bijhouden van een geactualiseerd overzicht van geregistreerde datalekken (inbreuken op de beveiliging).

4.4 Register van verwerkingsactiviteiten (registerplicht)

De verwerkersverantwoordelijke dient in het kader van zijn verantwoordingsplicht een register bij te houden van alle verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden (art.30, lid 1, Avg en art. 31d Wpg). Deze verplichting dient een goed inzicht en overzicht te bieden en vereist een vergaande inventarisatie en uitputtende registratie van alle verwerkingsactiviteiten. Bovendien is doorlopende aandacht voor het onderhouden en actualiseren van het register nodig.

De verwerkingsverantwoordelijke houdt een register bij van de verwerkingsactiviteiten die onder zijn verantwoordelijkheid plaatsvinden. Dat register bevat alle volgende gegevens:

- naam en contactgegevens van de verwerkingsverantwoordelijke en de Avg-coördinatoren en van de FG;
- de verwerkingsdoeleinden;
- een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- de categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt (incl.
- ontvangers in derde landen of internationale organisaties);
- voor zover van toepassing: doorgiften van persoonsgegevens aan een derde land of een internationale organisatie (artikel 49 lid1 Avg), de documenten inzake de passende waarborgen;
- indien mogelijk, de beoogde termijnen waar binnen de verschillende categorieën van gegevens moeten worden gewist;
- indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen als bedoeld in artikel 32 lid 1 Avg.

Voor de verwerkingsactiviteiten die onder de Wpg plaatsvinden geldt de registerplicht pas sinds 1 januari 2019. Omdat op dat moment het bij Defensie in gebruik zijnde Avg-verwerkingenregister nog niet geschikt was voor het invoeren van Wpg verwerkingsactiviteiten werd een tijdelijke technische voorziening, toegankelijk via Sharepoint, ingericht. De inventarisatie en registratie van de Wpg verwerkingen was in 2020 nog niet volledig uitgevoerd. Er wordt door de KMar op brigade en eenheidsnivo navraag en onderzoek gedaan om alle verwerkingsactiviteiten op proces- of systeemniveau te inventariseren en registreren. Dit zal naar verwachting pas in 2021 een completer beeld en overzicht opleveren. Op advies van de FG zullen alle in kaart gebrachte verwerkingsactiviteiten centraal worden opgenomen in het verwerkingenregister Defensie en komt de tijdelijke voorziening te vervallen. De hiervoor benodigde up-date/ systeemrelease is eind 2020 beschikbaar gekomen.

De FG heeft over 2020 bezien of de daadwerkelijk geregistreerde verwerkingen in register van verwerkingsactiviteiten valide, volledig en up to date zijn.

	CZSK	CLAS	CLSK	KMar Avg	KMar Wpg	BS	DMO/JIVC	DOSCO
		i	i	i	ii		i	i

Ja / goed	
Onvolledig	
Nee/onvoldoende	

Bevindingen:

i. Ondanks het feit, dat er inmiddels veel meer verwerkingen staan opgenomen in het Avg-verwerkingenregister, is bij de meeste defensieonderdelen de registratie nog niet volledig op orde.
Tevens staan veel verwerkingen nog 'in bewerking' en zijn nog niet gepubliceerd.
Aandachtspunt: *alle* verwerkingen van persoonsgegevens dienen volledig gedocumenteerd (voor zover relevant inclusief de DPIA en de verwerkingenovereenkomst) geregistreerd te zijn.

ii. De KMar is per 1 januari 2019 op grond van haar wettelijke verplichting gestart met inventariseren en registreren van de Wpg verwerkingen. Aangezien het Avg-verwerkingenregister van Defensie op dat moment nog niet aangepast en geschikt gemaakt was voor het registreren van Wpg verwerkingen is hiervoor een tijdelijke voorziening getroffen. Het voornemen is om het Avg verwerkingenregister vanaf 2021 te gaan vullen en ook alle Wpg verwerkingsactiviteiten hierin te registreren en de tijdelijke voorziening daarna op te heffen.

Aanbeveling:

Completeer en documenteer het Defensie verwerkingenregister (incl. DPIA's en verwerkersovereenkomsten) en bevorder het bijhouden van een geactualiseerd overzicht van geregistreerde datalekken (inbreuken op de beveiliging).

4.5 Verwerkersovereenkomsten

Wanneer het Ministerie van Defensie als verwerkingsverantwoordelijke (of een van de defensieonderdelen die zijn aangewezen als Avg- of Wpg-beheerder of -onderbeheerder) een andere overheidsinstantie of -dienst, een natuurlijke persoon of een rechtspersoon wil inschakelen om ten behoeve van Defensie persoonsgegevens te laten verwerken is er mogelijk sprake van een verwerkersrelatie.

Artikel 28 Avg en artikel 6c Wpg bepalen dat, wanneer door een verwerkingsverantwoordelijke een (technisch) verwerker wordt ingeschakeld hiervoor uitsluitend een verwerker mag worden ingeschakeld die afdoende garanties met betrekking tot de juiste toepassing van technische en organisatorische maatregelen biedt om de naleving van de Avg en de Wpg te kunnen waarborgen. Een en ander dient te zijn vastgelegd in een verwerkersovereenkomst (of andere rechtshandeling b.v. een convenant).

Op grond van artikel 1.4 Regeling Avg Defensie en artikel 1.5 van de regeling Wpg Defensie mogen Avg- en Wpg-beheerders of -onderbeheerder een dergelijke verwerkersovereenkomst sluiten.

Let wel: dit gaat uitsluitend om situaties waarbij een verwerker wordt ingeschakeld om persoonsgegevens in het belang van het organisatieproces van Defensie, in opdracht- en met strikte instructies van Defensie te gaan verwerken. Een verwerker mag op zijn beurt ook geen andere verwerker (sub verwerker) inschakelen zonder toestemming van Defensie. De verwerker bepaalt niet zelf het doel en de middelen van de verwerking. Als een ander overheidsdienst, persoon of rechtspersoon de persoonsgegevens gaat verwerken ten behoeve van het eigen organisatieproces en op basis van zelf bepaalde doelen en middelen dan is er geen sprake van een verwerkersrelatie maar is er sprake van individuele verwerkingsverantwoordelijken die onderling persoonsgegevens verstrekken en ontvangen maar waarbij geen sprake is van een verwerkersrelatie.

Voor 2020 is de verplichting tot het sluiten van verwerkersovereenkomsten op de volgende aspecten door de FG ter beoordeling bezien:

a. Wordt tijdig en op juiste wijze beoordeeld en vastgesteld of er sprake is van een verwerkersrelatie?
b. Is er een goed overzicht van verwerkersovereenkomsten die nog afgesloten of geactualiseerd dienen te worden?
c. Voldoen de gesloten verwerkersovereenkomsten of afspraken aan de wettelijke vereisten:

bevat ten minste afspraken over of verwijzingen naar:

- het onderwerp en de duur van de verwerking
- de aard en het doel van de verwerking
- het soort persoonsgegevens en de categorieën van betrokkenen
- strikte schriftelijke instructies onder andere voor wat betreft de doorgifte van persoonsgegevens aan derde landen of internationale organisaties
- autorisaties en geheimhoudingsplicht
- naleving en borging rechten betrokkenen
- naleving en procedureafspraken meldplicht datalekken
- het wissen/teruggeven van persoonsgegevens na einde overeenkomst
- inschakeling subverwerkers
- medewerking aan toezicht activiteiten en audits

d. Worden de verwerkersovereenkomsten toegevoegd aan het register van verwerkingsactiviteiten?

	CZSK	CLAS	CLSK	KMar AVG	KMar WPG	BS (apparaat)	BS DOPS	BS (defensiebreed)	DMO	DMO/ JIVC	DOSCO
a	i	i	i	i	i	i		i	i	i	i
b											
c	ii	ii	ii	ii	ii	ii		ii	ii	ii	
d											

Ja/goed	
Onvoldoende	
Nee	
Onbekend / geen info	
Niet van toepassing	

Bevindingen:

i. Er is behoefte aan eenduidig beleid en overzicht voor het beoordelen en wettelijk juist interpreteren van de relatie tussen Defensie en partijen waarmee wordt samengewerkt in het licht van de Avg en de Wpg. Het is van groot belang, dat gegevensbescherming prominent aan de voorkant van het inkoopproces (incl. beveiliging en ABDO) wordt meegenomen. Bovendien wordt het onderscheid tussen samenwerkingsrelaties vanuit ieders individuele verwerkingsverantwoordelijkheid, vanuit een gezamenlijke verwerkingsverantwoordelijkheid of op basis van verwerkersrelatie en –overeenkomst, niet in alle gevallen juist gemaakt. Hierdoor worden mogelijk verwerkersovereenkomsten afgesloten in situaties waarin dit niet noodzakelijk is en wordt de verwerkingsverantwoordelijkheid niet belegd bij de juiste partij.
ii. Over het verslagjaar 2020 zijn onvoldoende gegevens beschikbaar.

Aanbeveling:

Meer aandacht voor professionalisering van de Avg/Wpg-functie en investeer op deze wijze in het vergroten van het kennisniveau.

Meer aandacht voor de beveiliging van persoonsgegevens bij de uitwisseling ervan met externe partijen en investeer in het verhogen van de bewustwording (inkoopketen).

Completeer en documenteer het Defensie verwerkingenregister (incl. DPIA's en verwerkersovereenkomsten) en bevorder het bijhouden van een geactualiseerd overzicht van geregistreerde datalekken (inbreuken op de beveiliging).

4.6 Rechten van betrokkene

De Algemene verordening gegevensbescherming (Avg) kent aan betrokkenen privacyrechten toe. Daartoe is in de aanloop van de inwerkingtreding van de Avg een proces rechten betrokkenen ingericht. Een vergelijkbare regeling is ook in de Wpg voorzien. Hierop gelden echter wel specifieke uitzonderingen die het recht van de betrokkene kunnen beperken als dat nodig is. Bijvoorbeeld wanneer het in het belang van de openbare orde en veiligheid of om belemmering de politietaak of strafrechtelijke onderzoeken te voorkomen.

Betrokkene

Een betrokkene is een natuurlijk persoon van wie persoonsgegevens worden verwerkt. Alle informatie die betrekking heeft op een geïdentificeerde of identificeerbare natuurlijke persoon, wordt als persoonsgegevens beschouwd. De rechten kunnen ook namens betrokkene worden uitgeoefend bijvoorbeeld door een advocaat.

Rechten

Betrokkene heeft de volgende rechten:

- Recht op **informatie/recht op inzage** (artikel 15 Avg, artikel 24a, 24b en 25 Wpg)
- Recht op **rectificatie** (artikel 16 Avg, artikel 28 Wpg)
- Recht op **gegevenswissing** -recht op vergetelheid- (artikel 17 Avg, geen Wpg-recht)
- Recht op **beperking van de verwerking** (artikel 18 Avg, geen Wpg-recht)
- Recht op **overdraagbaarheid gegevens** -dataportabiliteit- (artikel 20 Avg, geen WPG-recht)
- Recht van **bezwaar** (artikel 21 Avg)
- Recht op **menselijke tussenkomst** bij geautomatiseerde besluitvorming waaronder profilering (artikel 22 Avg, 7a Wpg)

Het recht op vergetelheid en dataportabliteit zijn ‘’nieuwe’’ rechten van de Algemene verordening gegevensbescherming (Avg); de andere rechten bestonden al onder de Wet bescherming persoonsgegevens (Wbp). Betrokkenen kunnen hun rechten alleen doen gelden op hun *eigen* persoonsgegevens. En dus niet op persoonsgegevens van anderen. Dit was onder de Wbp niet anders en geldt ook bij WOB-verzoeken.
Voor het indienen van een verzoek om privacyrechten is een proces rechten betrokkenen ingeregeld:
https://www.defensie.nl/onderwerpen/privacyrechten/privacyrechten-bij-defensie

Externe verzoeken van betrokkenen worden via de internetsite www.defensie.nl naar de juiste behandelaar geleid, zodat verzoeken tijdig en zorgvuldig worden behandeld. Voor medewerkers in werkelijke dienst geldt een vergelijkbaar proces via de intranetpagina privacy en beveiliging.
De meeste betrokkenen doen een beroep op het recht op informatie uit personeelsdossiers als onderdeel van stamboomonderzoek. In het jaar 2020 is ter beperking van de werklast een specificatie aangebracht bij personeelsdossiers (volledig personeelsdossier en overzicht staat van dienst) en medische dossiers. Gedurende de coronacrisis is een significante stijging van het aantal verzoeken waargenomen. Naast bovengenoemde gegevens moet ook vermeld worden, dat ondanks het feit, dat verzoeken ten aanzien van privacyrechten via het centrale proces dienen te lopen, komen er ook talrijke verzoeken binnen bij de Avg coördinatoren van de defensieonderdelen.

Avg klachten/vragen/signalen

Enkele van de vele externe verzoeken hebben geleid tot vragen, veroorzaakt door een vertraagde afhandeling of onduidelijke vraagstelling. Deze vragen zijn op enkele casussen na afgehandeld.
De FG behandelt zelf geen klachten. Wel zien zij toe op de afhandeling van Avg/Wpg-klachten door de beheerders. Soms komen er toch klachten bij de FG binnen. Deze worden dan aan de verantwoordelijke beheerder doorgezonden. In 2020 zijn enkele klachten door de FG ontvangen en in samenspraak met de Juridische Dienstverlening (JDV) en de desbetreffende Avg-coördinator afgehandeld. Opvallend is daarin de toename aan gecombineerde Avg/WOB verzoeken.

Privacyverklaring

De privacyverklaring is opgenomen op zowel het internet als het intranet van Defensie en andere websites waar persoonsgegevens met Defensie als uitvoeringsverantwoordelijke worden verwerkt (zoals www.rijksoverheid.nl, www.defensie.nl en www.werkenbijdefensie.nl). In deze privacyverklaring is beknopt, transparant en in duidelijke en eenvoudige taal en in een gemakkelijk toegankelijke vorm beschreven welke gegevens worden verwerkt en op welke wijze de betrokkenen hun rechten kunnen uitoefenen. In de privacyverklaring wordt specifieke aandacht besteed aan de toepassing van de WPG op de verwerking van persoonsgegevens bij de KMar.

Overig; meldingen vrijgave account

In geval van overlijden van een medewerker of een ander zwaarwegend belang (bijv. bij langdurige ziekte van een medewerker), kan het voorkomen dat het noodzakelijk is om, met ondersteuning van JIVC, toegang te verschaffen tot het digitale account van betrokkene. Hiervoor moet dan door de betreffende Beveiligingscoördinator (BC) toestemming worden verleend. De daadwerkelijke vrijgave vindt vertrouwelijk plaats met gebruikmaking van een two mans concept. Van een dergelijke toestemming wordt melding gemaakt bij de FG. In 2020 zijn er 3 van dergelijke meldingen door de FG ontvangen.

4.7 Meldplicht Datalekken/inbreuk op de beveiliging

Datalekken worden, zoals beschreven in de (herziene) SG aanwijzing 005, gemeld in het Melding Voorvallen-systeem (MVV-systeem). De Avg-coördinator of privacyfunctionaris beoordeelt het datalek conform de procedure en consulteert de FG. De tooling die wordt gebruikt voor het MVV loopt echter nog niet synchroon met de te melden Avg voorvallen/datalekken. Veelal worden deze in het MVV systeem gemeld als zijnde een beveiligingsincident of integriteitskwestie (* bijzondere gebeurtenis), waardoor de wettelijke termijn (binnen 72 uur) om een datalek te melden bij de Ap vaak niet wordt gehaald . Het verdient aanbeveling de MVV tooling hierop aan te passen.

De meldplicht voor datalekken dateert uit 2016 en is in versoepelde vorm opgenomen in de Avg en sinds 2019 ook in de Wpg. De term datalek werd in artikel 34a Wbp uitgelegd als *'een inbreuk op de beveiliging, bedoeld in artikel 13, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens'*. In artikel 33 Avg en 33a Wpg wordt een bij de Ap meldingsplichtig datalek omschreven als: 'een inbreuk in verband met persoonsgegevens, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.' Het beoordelen (ofwel het 'wegen') door de Avg-coördinator of een datalek dient te worden beschouwd als een bij de Ap meldingsplichtig datalek is derhalve juridisch gecompliceerd.

In 2020 zijn door Defensie in totaal 15 datalekken in het kader van de Avg en 0 datalekken in het kader van de Wpg gemeld bij de Ap. Dit is een (geringe) afname ten opzichte van de datalekken die de afgelopen jaren aan de Ap zijn gemeld. Voor wat betreft de 'interne' datalekken (de niet bij de Ap meldingsplichtige datalekken) zien we daarentegen een toename.
In het MVV-systeem worden ook voorvallen gemeld, die aan de Avg raken.
De Avg is in het MVV-systeem dan ook een bijzondere categorie, die door de melder expliciet aangevinkt kan worden. De FG ontvangt een afschrift van de zodanig gekwalificeerde meldingen. Deze meldingen worden door de FG aangemerkt als een signaal en kunnen (mede) als basis dienen voor nader toezicht. Dan dient het wel te

gaan om een structurele misstand en niet om een op zichzelf staand incident.
In 2020 zijn 156 van dergelijke meldingen door de FG ontvangen. Dat is beduidend hoger dan het aantal MVV meldingen het jaar daarvoor, terwijl ook toen al een stijging waarneembaar was ten opzichte van de jaren daarvoor (zie overzicht hieronder). In geen van de gevallen heeft de melding geleid tot het instellen van nader toezicht. De bovengenoemde stijging van het aantal MVV-meldingen kan gedeeltelijk verklaard worden door het toegenomen privacybewustzijn van de medewerkers waardoor MVV-meldingen, die voorheen uitsluitend als een beveiligingsincident werden aangemerkt, nu vaker ook als Avg-incident worden gezien. Veel meldingen werden gedaan na telefoontjes vanuit het buitenland, phishing mails, openstaande Sharepoint of het hacken van een Facebookaccount.

	2020	2019	2018	2017	2016	2015	2014
Avg gerelateerde MVV meldingen	156	95	75	51	49	37	23
Bij Ap (extern) gemelde datalekken	15	14	16	18	17	0	0
Wpg gerelateerde MVV meldingen	5	9	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Bij Ap (extern) gemelde datalekken	0	1	n.v.t.	n.v.t.	n.v.t.	n.v.t.	n.v.t.
Totaal	**172**	**104**	**90**	**69**	**66**	**37**	**23**

4.8 Audits

De verwerkingsverantwoordelijke moet kunnen aantonen dat de verwerking van persoonsgegevens in overeenstemming met de Avg en de Wpg wordt uitgevoerd. Vanuit de wetgeving ligt de nadruk daarom niet alleen op het naleving en waarborging (compliance) maar geldt nadrukkelijk ook een verantwoordingsplicht (accountability). Met andere woorden het gegevensbeschermingsrecht moet niet alleen worden toegepast en nageleefd, de naleving moet ook aantoonbaar zijn.

Naast de toezichthoudersrol van de FG en het externe toezicht door de Autoriteit persoonsgegevens is het (laten) uitvoeren van audits een belangrijk instrument hiervoor. Dit kan gaan om interne- of externe Electronic Data Processing (EDP) audits of IT-audits. De uitvoering van audits is in beginsel optioneel en zonder vaste normering opgenomen in de Avg. De Avg bevat eigenlijk een audit recht dat de verwerkingsverantwoordelijke met name in staat stelt om aan zijn verantwoordingsplicht te kunnen voldoen en om de nakoming van afspraken met verwerkers (neergelegd in verwerkersovereenkomsten) te controleren middels audits (artikel 24 en 28 lid 3 h Avg).

In artikel 7 van de Regeling Avg Defensie is opgenomen dat de Audit Dienst Rijk (ADR), al dan niet op verzoek van de FG of een Avg-beheerder (periodiek) audits kan laten uitvoeren naar de naleving van de Avg.

De Wpg kent in tegenstelling tot de Avg wél een auditverplichting op grond van artikel 33 Wpg die nader uitgewerkt is in het Besluit politiegegevens en de Regeling periodieke audit politiegegevens[3]. Deze verplichting houdt in dat via interne én via externe audits controles dienen te worden uitgevoerd naar opzet, bestaan en werking van de organisatie en de genomen maatregelen en procedures rond de naleving van de Wet

[3] in werking sinds 1 januari 2009 zie Staatscourant 2008 nr. 252, laatstelijk gewijzigd 21 juni 2019, Staatcourant 2019 nr. 31163

politiegegevens. Deze audits dienen jaarlijks intern plaats te vinden op deelaspecten van de Wpg en eenmaal per 4 jaar dient een volledige en onafhankelijke externe audit te worden uitgevoerd door de ADR. Bij tekortkomingen dienen op basis van een verbeterplan maatregelen te worden genomen en volgt binnen 1 jaar hercontrole.

Voor 2020 is de uitvoering van de Wpg-audits op de volgende aspecten door de FG ter beoordeling bezien:

a. Is de organisatie bekend met de mogelijkheid dan wel de verplichting tot het uitvoeren van audits?
b. Is er voldoende interne en externe (Adr) capaciteit beschikbaar voor het uitvoeren van de audits?
c. Is er een interne of externe Avg-audit uitgevoerd naar de naleving van de Avg of Wpg?
d. Is de periodiek verplichte (jaarlijks) interne Wpg audit uitgevoerd?
e. Is de laatste periodiek verplichte (4-jaarlijkse) externe Wpg audit uitgevoerd?
f. Is er een plan van aanpak verbetermaatregelen opgesteld en is de verplichte hercontrole uitgevoerd?

	CZSK	**CLAS**	**CLSK**	**KMar Avg**	**KMar Wpg**	**BS (apparaat)**	**BS (defensiebreed)**	**DMO**	**DMO/ JIVC**	**DOSCO**
a										
b					i					
c	i	i	i	i	ii	i	i	i	i	i
d					ii					
e					ii					
f					ii					

Ja/goed	
Onvoldoende	
Nee	
Onbekend	
Niet van toepassing	

Bevindingen:

i. De Avg-beheerders van de defensieonderdelen hebben 2020 geen audits laten uitvoeren. In 2020 heeft de ADR wel een rijksbrede audit uitgevoerd (rechten betrokkenen en inrichting register van verwerkingsactiviteiten).
ii. De privacyfunctionaris heeft in 2020 intern onderzoek uitgevoerd naar de Wpg-compliance over de periode 2014-2018. In het derde kwartaal van 2020 is het rapport opgeleverd en gedeeld met de ADR. De ADR voert, mede op basis van deze uitkomsten in 2021 de wettelijk verplichte externe audit uit. In 2020 is een Audit coördinator aangenomen ter uitvoering van de verplichte interne WPG- audits voor de periode 2019-2022.

Aanbeveling:

Voldoende capaciteit en middelen ter professionalisering van de Avg/Wpg functie en investeer op deze wijze in het vergroten van het kennisniveau van de Avg/Wpg.

5. Overige toezichtwerkzaamheden

Toezichtbezoek Kustwacht Nederland

In 2020 is de Kustwacht Nederland bezocht in het kader van implementatie van de Avg en Wpg. In 2020 is een begin gemaakt met het in gezamenlijkheid met de Avg coördinator CZSK oplopen van plan van aanpak hieromtrent (blauwdruk nulmeting). In april 2021 zal het plan van aanpak worden opgeleverd en geïmplementeerd binnen de Kustwacht Nederland.

Onderzoek Chroomhoudende verf en Chemical Agent Resistant Coating (Chroom-6 en CARC)

In het kader van het onderzoek naar gezondheidsklachten van (oud) medewerkers van Defensie, die zij aan het werken met chroomhoudende verf en Chemical Agent Resistant Coating (CARC) toeschrijven, is samen met de BA de afgelopen jaren intensief toezicht op de verwerking van persoonsgegevens en de beveiliging daarvan bij het ingerichte informatiepunt uitgevoerd. Dit informatiepunt is ingericht door en valt onder verantwoordelijkheid van het Centrum Arbeidsverhoudingen Overheids Personeel (CAOP), een faciliterende stichting waarmee Defensie voor de ondersteuning van de uitvoering van het onderzoek een contract heeft gesloten. Het toezicht op de beveiliging van persoonsgegevens bij het onder CAOP vallende informatiepunt vindt plaats op grond van de verwerkersovereenkomst met Defensie, waarbij bij het CAOP tweemaal per jaar toezicht wordt uitgevoerd. Eerder is reeds vastgesteld dat het CAOP grotendeels voldoet aan de vastgestelde beveiligingsnormen zoals beschreven in de Avg en de Baseline Informatiebeveiliging Rijksdienst (BIR) en is in 2020 geconstateerd dat de verbetermaatregel om te komen tot een DPIA, afronding nadert. Aandachtspunten zijn, naast actualisatie van de DPIA, actualisatie van de verwerkersovereenkomsten met (sub)verwerkers. Deze constatering in combinatie met de aangescherpte COVID-19 maatregelen heeft de FG in overleg met de BA doen besluiten het (intensieve) toezichttraject af te sluiten en over te gaan naar een reguliere invulling van de toezichtrol.

Defensie Ondersteunings Commando (DOSCO)

Bijzondere aandacht voor DOSCO als ‘persoonsgegevens zwaar’ defensie onderdeel. Zo onderkennen we binnen DOSCO onder meer de zorgeenheden, geestelijke verzorging, internationale gegevensoverdracht, onderzoek en personeelszorg (en de daaraan gerelateerde inkooporganisatie). De afgelopen jaren is bij eenheden ressorterende onder de divisie Defensie Gezondheidszorg Organisatie (DGO), zoals het Centraal Militaire Hospitaal (CMH), een grote achterstand in de naleving van de Wbp (voorloper van de Avg) geconstateerd. De beveiliging (art. 32 Avg) bij gegevensuitwisseling met zorgverleners in de civiele sector (ziekenhuizen, tandartsen, onderzoekscommissies etc.) bleek niet altijd op orde en verdient daarom aandacht. Medio 2020 heeft een (digitaal) toezichtbezoek aan Staf DGO plaatsgevonden, waarbij is geconstateerd dat veel van de achterstand is ingelopen het afgelopen jaar. FG blijft hier, ook de komende jaren, op toezien.

Onderzoeken

Incidentonderzoeken naar inbreuken in verband met persoonsgegevens en inbreuken op de beveiliging (datalekken) zijn in 2020 toegenomen, vooral in verband met de

verwerking van persoonsgegevens betreffende de gezondheid. Daarnaast heeft de FG in 2020 een intern toezichtonderzoek geïnitieerd naar de naleving van de Avg in relatie tot de verwerkingsactiviteiten die zijn verricht door de experimenteeromgeving Land Information Manoeuvre Centre (LIMC) binnen de Koninklijke Landmacht. Het onderzoek zal in het 1e kwartaal 2021 worden afgerond met een rapportage die zal worden aangeboden aan Avg beheerder van de Koninklijke Landmacht en de Minister van Defensie als verwerkingsverantwoordelijke.

Tot slot

Gedurende 2020 (maart-december) golden COVID-19 maatregelen . De beperkende maatregelen (gelet op toezichtbezoeken /interviews/ werken op afstand) zijn van grote invloed geweest op de (niet uitputtende) uitvoering van het FG-toezichtjaarplan 2020.

6. Samenwerking

Bij het uitoefenen van de functie heeft de FG in 2020 nauw samengewerkt met diverse functionarissen, organisatieonderdelen en overlegstructuren, zowel binnen als buiten de defensieorganisatie.

Interne samenwerking

Binnen Defensie heeft de FG in het kader van haar toezichthoudende taak, nauw contact met de Avg-coördinatoren als eerste contactpersoon bij de diverse defensieonderdelen. Hierbij geeft de FG, mits de toezichthoudende rol hiermee niet in het gedrang komt, ook incidenteel advies.

Vanuit de BS/DBE/Avg coördinatie is een bijdrage geleverd aan de totstandkoming van een rijksbrede handreiking naleving Avg.
https://intranet.mindef.nl/bs/Images/JenV%20handreiking%20naleving%20AVG_WEB%20vastgestelde%20versie%20ICBR%20030620_tcm4-1464320.pdf

Begin december 2020 heeft voor de Avg coördinatoren een (digitale) DPIA bijeenkomst plaatsgevonden.

DJZ is belast met de tweedelijns juridische advisering, inzake defensie brede beleidsvorming en juridische advisering omtrent vraagstukken van (politiek) principiële aard, ook ten aanzien van onderwerpen die raken aan de bescherming van persoonsgegevens. Ook in 2020 heeft de FG herhaaldelijk contact gehad met DJZ, met name op het gebied van opstelling en wijziging van de Regeling Gegevensbescherming Militaire Operaties, de aanpassing van de Regeling Wpg Defensie en bijdragen aangaande de evaluatie van de Avg.

Daar waar, in concrete situaties, de bescherming van de persoonsgegevens en de openbaarheid van bestuur elkaar raakten, is in 2020 door de FG enkele malen samengewerkt met de WOB-coördinator van het Ministerie van Defensie.

Aangezien het toezichtdomein voor wat betreft de Avg veel raakvlakken heeft met andere (toezicht) domeinen, zoals integriteit, documentaire informatievoorziening & beveiliging zijn het afgelopen jaar de samenwerkingsverbanden ook op die vlakken geïntensiveerd. Tevens is, naast de bijdrage van de BA aan het kernteam betrokken bij het onderzoek naar de verwerkingsactiviteiten bij LIMC, ook aansluiting en ondersteuning gezocht bij de IVD als coördinerend toezichthouder. Dit betreft zowel organisatorische, juridische als facilitaire ondersteuning.

De toezichthouders overleggen (minimaal) halfjaarlijks onder leiding van de Inspecteur-Generaal Veiligheid in het zogenaamde Toezichtberaad. In 2020 is het Toezichtberaad frequenter bijeengekomen. Tevens hebben in het kader van verbetering van de samenhang en kwaliteit in het toezicht binnen Defensie onder voorzitterschap van AEF (Andersson Elffers Felix) een aantal besprekingen plaatsgevonden.

Externe samenwerking

De FG werkt, om zijn taak goed uit te kunnen voeren, ook samen met personen en instanties buiten de defensieorganisatie.
In 2020 heeft meerdere malen contact plaatsgevonden tussen de FG en medewerkers van de Autoriteit persoonsgegevens (Ap).

ADR

De ADR heeft evenals voorgaande jaren een Rijksbreed Avg onderzoek gedaan. In 2020 is er vooral gekeken naar invulling door het departement van de rechten van betrokkene,

het register van verwerkingsactiviteiten en de opvolging van de aanbevelingen voortkomend uit het rijksbrede Avg onderzoek 2019.

Internationale samenwerking/Marshall Center

In het kader van internationale samenwerking op het gebied van gegevensbescherming zijn er in 2020 (digitale) initiatieven geweest waar de FG's aan hebben deelgenomen. Vermeldenswaard in dit verband is de eerste Military and National Security Data & information protection (virtual) workshop die in juni en september 2020 heeft plaatsgevonden. Een internationale bijeenkomst over gegevensbescherming en privacy in militaire context, georganiseerd door het George C. Marshall Centre in Garmisch-Partenkirchen. Aan de virtuele sessie werd deelgenomen door vertegenwoordigers vanuit Duitsland, Frankrijk, Portugal, Denemarken, Ierland, de VS en de NAVO. Op de agenda stond de nadere inventarisatie en uitwerking van de wettelijke kaders en actuele implementatievraagstukken van de deelnemende landen. En er zijn actuele vraagstukken en recente ontwikkelingen besproken aangaande het gegevensbeschermingsbeleid dat zich vanuit de operationele commandostructuur van de NATO aan het ontwikkelen is. Zeer waarschijnlijk zal medio 2021 een vervolgbijeenkomst worden gepland, virtueel of op de locatie in Garmisch-Partenkirchen.

Het RPFG

De voor de FG belangrijkste externe samenwerking vindt plaats in het Rijksplatform van Functionarissen voor de Gegevensbescherming (RPFG). Dit is het overleg van de FG's van de ministeries en enkele rijksbrede organisaties (ACM, Nationale Politie en CBS). Het belang van het RPFG is, gezien het toenemende aantal rijksbrede initiatieven en shared service voorzieningen, waarbij ook persoonsgegevens worden verwerkt, aanzienlijk toegenomen. Het RPFG wordt steeds meer een gesprekspartner in allerlei rijksbrede trajecten. Daarnaast is binnen het RPFG afgestemd over de invulling die is gegeven aan de Privacy Advies Functie Rijk (PAR) bij BZK, het huidige format voor een data protection impact assessment (DPIA) en het in gebruik genomen Avg-verwerkingenregister.

RPFG voor Wpg en Wjsg

In samenwerking met de FG van de Politie is het initiatief genomen een platform of netwerkorganisatie op te richten voor Functionarissen voor Gegevensbescherming die zijn aangesteld op grond van de Wpg en Wjsg. Dit platform is in 2020 voor het eerst virtueel bijeengekomen.

Bijlage A: Toezichtjaarplan FG 2020

Planning toezichtbezoeken 2020

CZSK / Kmar : Kustwacht	Q1
KMar / STC / DB / IV&C : 32a Wpg loggingsverplichtingen en autorisatiebeheer	Q1 / Q2
DOSCO: IDR (zorgopleidingen); CMH / UMCU : doorlopend; CIOD; DCPL	Q2
CLAS: JISTARC	Q2
BS/HDP: Stichting Veteraneninstituut	Q3
BS / CZSK / KMar : Gegevensuitwisseling binnen CARIB-NL (derde landen/BES)	Q2 / Q4
KMar / LTC / SPL : werking Frontoffice Pi-NL	Q3
BS / HDP: CAOP/RIVM ihkv o.a. het Chroom 6 & CARC onderzoek	Q2 / Q4
BS / HDP: VGZ bedrijven (irt SZvK)	Q3 / Q4

Bijlage B: Speerpunten voor 2021 (toezichtjaarplan FG 2021)

De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld. Persoonsgegevens doorgeven vanuit Nederland naar het buitenland mag daarom alleen als een land voldoende bescherming biedt. Voor doorgifte van gegevens naar een land binnen de Europese Unie (EU) gelden andere regels dan voor doorgifte naar een land buiten de EU, zowel in de Avg als in de Wpg.

Voor doorgifte van persoonsgegevens vanuit Nederland naar landen buiten de EU, zogeheten derde landen, gelden aparte regels.

De hoofdregel is, dat een organisatie persoonsgegevens alleen mag doorgeven naar derde landen met een passend beschermingsniveau. In dit verband worden de overige landen binnen het Koninkrijk Nederland (Curaçao, Aruba, St. Maarten) ook als derde landen beschouwd. Dit geldt ook voor in Nederland gevestigde internationale (militaire) organisaties waarmee persoonsgegevens worden uitgewisseld.

Evenals gegevensuitwisseling met (sub)verwerkers ontstaan er risico's ten aanzien van persoonsgegevens indien deze worden uitgewisseld met derde landen of internationale organisaties zonder passend beschermingsniveau. Om deze reden zal het FG toezicht in 2021/2022 mede in het teken staan van deze internationale gegevensuitwisseling.

In 2021 zal het toezicht van de FG's zich richten op internationale gegevensuitwisseling en op verwerkingen van persoonsgegevens door (sub)verwerkers.

Naast de regulier uit te voeren toezichtwerkzaamheden zal eveneens aansluiting worden gezocht bij de focusgebieden van de Autoriteit persoonsgegevens (de nationale toezichthouder) te weten: datahandel, digitale overheid en artificiële intelligentie en algoritmes, die voor de periode 2020 tot en met 2023 zijn aangewezen in het visiedocument 'Dataprotectie in een digitale samenleving'.
Ook deze focusgebieden krijgen de komende jaren aandacht in ons toezicht.

Om de effectiviteit van het toezicht te vergroten wordt ook in 2021 heel nadrukkelijk aansluiting gezocht bij toezichtpartners binnen Defensie, zoals de IMG, IVD en de Beveiligingsautoriteit (BA). Binnen het Toezichtsberaad is afgesproken, dat deze samenwerking zal worden geïntensiveerd en dat ook samenwerking met andere interne toezichthouders zal worden gezocht. Dit zal vooral zichtbaar zijn in het (evenals in voorgaande jaren) afleggen/combineren van toezichtbezoeken.

Tevens zal internationale samenwerking worden gezocht met de FG's van de Ministeries van Defensie van de ons omringende EU-landen om te bezien of er samenwerkingsverbanden mogelijk zijn, die een passend beschermingsniveau kunnen bieden voor internationale gegevensverwerking (verstrekking).

Sinds 2019 heeft Defensie ook een Functionaris voor Gegevensbescherming vanuit de Wpg. Voor zover een duidelijk onderscheid te maken valt in te bezoeken eenheden zal op die plaatsen gesproken worden van een FG Avg en een FG Wpg. Aangezien de werkvelden veel met elkaar te maken hebben kunnen toezichtbezoeken in gezamenlijkheid worden afgelegd. De ontvlechting van datastromen vraagt extra aandacht nu de vreemdelingentaken van de KMar onder het huidige wettelijke regime niet langer onder de Wpg, maar onder de Avg zijn komen te vallen. Dit heeft gevolgen voor een aantal werkprocessen en automatiseringssystemen.

Medio 2019 is onder politieke en maatschappelijke belangstelling de Passenger Information Unit Nederland (Pi-NL) opgestart. Luchtvaartmaatschappijen zijn verplicht om bij vluchten binnen en buiten de EU de reserverings- en check-in gegevens van hun passagiers tijdig voor vertrek aan de bevoegde autoriteiten op de luchthavens te verstrekken. Het doel is het voorkomen en opsporen van terrorisme en ernstige criminaliteit. Pi-NL is een zelfstandige eenheid met eigen wettelijke taken en bevoegdheden onder de werkingssfeer PNR-richtlijn en de Wet passagiersgegevens. Op de verwerking van persoonsgegevens door Pi-NL is de Wpg (deels) van overeenkomstige toepassing verklaard. De Pi-NL eenheid valt onder het gezag van de Minister van Justitie en Veiligheid (NCTV) maar is beheersmatig ondergebracht bij Defensie. In de Pi-NL werken Politie, Openbaar Ministerie en KMar met elkaar en met bevoegde autoriteiten in andere lidstaten samen. Ten behoeve van de toegang tot en geautomatiseerde vergelijking van passagiersgegevens met politiegegevens is er een Pi-NL front-office ingericht bij de KMar. Vanwege de omvang, complexiteit en de gevoeligheid is de verwerking van PNR data binnen PI-NL en de frontoffice als speerpunt voor het FG Wpg toezicht aangemerkt in 2020.


Impact op productiviteit
44%
17%
17%
40%
38%
48%
45%
29%
41%
Comment
Fill & Sign
Move Redo
cmd

Planning toezichtbezoeken 2021

KMar / STC / DB / IV&C : 32a Wpg loggingsverplichtingen en autorisatiebeheer	Q1 / Q2
DOSCO : CMH / UMCU doorlopend; CIOD; DCPL	Q2
CLAS : JISTARC	Q1
BS / HDP : Stichting Veteraneninstituut	Q3
BS / CZSK / KMar : Gegevensuitwisseling binnen CARIB-NL (derde landen / BES)	Q2 / Q4
KMar / LTC / SPL : werking Frontoffice Pi-NL	Q2
BS / HDP : CAOP / RIVM ihkv o.a. het Chroom 6 & CARC onderzoek	Q2 / Q4
BS / HDP : VGZ bedrijven (irt SZvK)	Q3 / Q4
KMar : LTC / OPSCENT	Q3 / Q4