Ministerie van Volksgezondheid,
Welzijn en Sport

Jaarverslag FG VWS 2019-2020

Functionaris voor gegevensbescherming

Colofon

Secretaris Generaal / plv. Secretaris Generaal
Directie Bestuurlijke en Politieke Zaken

Bezoekadres:
Parnassusplein 5 2511 VX Den Haag

Contactpersoon H. Westerling - Woltman
Functionaris voor Gegevensbescherming

5.1.2e @minvws.nl

Versie	Definitief
Auteur	H. Westerling - Woltman
Bijlage(n)	1
Datum vaststelling	20 april 2021
Aantal pagina's	16

Managementsamenvatting

Dit jaarverslag van de Functionaris voor Gegevensbescherming (FG) gaat over de jaren 2019 en 2020. Waarbij het jaar 2019 een interessant vervolg was op het eerste jaar van de inwerkingtreding van de (U)AVG. Het jaar 2020 kenmerkte zich als een bijzonder jaar waar we in een andere werkelijkheid leven door de coronacrisis waarin wij ons bevinden. Een jaar waarin VWS een spin in het web was en is in de aanpak van de coronacrisis. Met deze crisis gingen nieuwe verwerkingen met grote stromen van gegevens gepaard, denk bijvoorbeeld aan de verschillende ontwikkelde apps, het vaccinatieregister als wel gegevens ten behoeve van monitoring en evaluatie. De nadruk van dit jaarverslag ligt daarom op het jaar 2020.

In de AVG zijn de belangrijkste regels neergelegd voor het verwerken van persoonsgegevens. Met de komst van de AVG is de noodzaak voor het afleggen van verantwoording in het kader van privacybescherming toegenomen. De AVG legt de nadruk namelijk op de verantwoordelijkheid van de organisatie om te kunnen aantonen dat zij zich houden aan de wet. Door te voldoen aan haar verantwoordingsplicht (accountability) levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

De FG houdt binnen VWS toezicht op de naleving van de AVG. Het toezicht van de FG is erop gericht om te verzekeren dat de minister voldoet aan zijn verplichtingen wat betreft het fundamentele recht op bescherming van persoonsgegevens. Een keer per twee jaar stelt de FG een jaarverslag op. Dit is geen verplichting maar draagt bij aan het bewust en zorgvuldig omgaan met persoonsgegevens binnen het ministerie.

De bevindingen wijzen uit dat het ministerie hard heeft gewerkt aan de bescherming van persoonsgegevens die het ministerie onder haar hoede heeft. Belangrijke punten van aandacht en prioriteit blijven: het kwalitatief goed uitvoeren van privacy impact assessments, het actueel houden van het AVGregister en de inzet van privacy adviseurs dan wel privacy officers bij voorgenomen verwerkingen van persoonsgegevens.

Het advies is om blijvend aandacht te besteden aan privacy by design bij de inrichting van werkprocessen, informatiesystemen en ketensamenwerkingen. Dit door aandacht te besteden aan de inzet van privacy by design, de kennis en de kunde van de medewerkers op dit onderwerp te vergroten, beleid hieromtrent te ontwikkelen en in de organisatie uit te rollen.

In 2019 en 2020 zijn door de FG tientallen adviezen bij verwerkingen van persoonsgegevens gegeven. De adviezen waren zeer divers, van het toetsen van de grondslagen bij een verwerking tot aan meer procesmatig als hoe om te gaan met gepseudonimseerde gegevens. Maar ook beleids, wet en regelgeving voorbereidende adviezen. Daarnaast heeft de FG in totaal 78 FG adviezen (33 in 2019 en 44 in 2020) op DPIA's uitgebracht. Enkele thema's komen vaker terug zoals de wettelijke grondslag waarop persoonsgegevens verwerkt mogen worden, het definiëren van verwerkingsverantwoordelijke versus verwerker, als wel de scope van de verwerking in relatie tot andere betrokken partijen.

De rode draad bij de adviezen betreft vooral het scherp krijgen van de grondslag waarop de persoonsgegevens verwerkt worden, de afweging van het nut en noodzaak van het gebruik van de gegevens en het stimuleren van de inzet van privacy by design bij een verwerking. Door enkel die persoonsgegevens te verwerken die daadwerkelijk nodig zijn, worden de privacy risico's verkleind.

Inhoud

	Managementsamenvatting	3
	Voorwoord	5
1	**Algemeen**	**6**
1.1	Inleiding	6
1.2	Leeswijzer	6
1.3	Persoonsgegevens en privacywetgeving	6
1.4	Hoe is privacy in de organisatie belegd?	6
2	**Werkzaamheden 2019 en 2020**	**8**
2.1	Coronacrisis	8
2.2	Gegevensbeschermingseffectbeoordeling (GEB-PIA, hierna DPIA)	8
2.3	Adviezen door de FG	10
2.4	Meldplicht datalekken	10
2.5	FG contacten met de burger	11
2.6	FG contacten met de AP	12
2.7	Voorlichting	12
2.8	Overleggremia	12
3	**Ontwikkelingen en vooruitblik**	**14**
3.1	Ontwikkelingen	14
3.2	Privacy by Design	14
3.3	Vooruitblik	15
	Bijlage: Afkortingen	**16**

Voorwoord

Dit jaarverslag van de Functionaris voor gegevensbescherming (FG) gaat over de jaren 2019 en 2020. Waarbij het jaar 2019 een interessant vervolg was op het eerste jaar van de (U)AVG. Waarbij 2020 zich kenmerkt als een bijzonder jaar waarin we in een andere werkelijkheid leven door de coronacrisis waarin we ons bevinden. Wat betekent dat we met z'n allen thuiswerken, er geen fysiek overleg is en we op een andere manier samenwerken.

Een jaar ook waarin VWS een spin in het web was en is in de aanpak van de coronacrisis. Met deze crisis gingen nieuwe verwerkingen en grote stromen van gegevens gepaard, denk bijvoorbeeld aan de verschillende ontwikkelde apps, het vaccinatieregister als wel gegevens ten behoeve van monitoring en evaluatie. De nadruk van dit jaarverslag zal daarom liggen op het jaar 2020.

In de AVG zijn de belangrijkste regels neergelegd voor het vastleggen en gebruiken van persoonsgegevens. Met de komst van de AVG is de noodzaak voor het afleggen van verantwoording in het kader van privacybescherming toegenomen. De AVG legt de nadruk namelijk op de verantwoordelijkheid van de organisatie om te kunnen aantonen dat ze zich houden aan de wet. Door te voldoen aan haar verantwoordingsplicht (accountability) levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Organisaties dienen inzichtelijk (transparant) aan te geven welke (persoons)gegevens zij verwerken en voor welk doel. Verder mogen niet meer gegevens worden verwerkt en niet langer bewaard dan strikt noodzakelijk is. Bovendien moet een organisatie passende beveiligingsmaatregelen treffen.

Onder de verantwoordelijkheid van de minister van Volksgezondheid, Welzijn en Sport (VWS) vindt een groot aantal verwerkingen van persoonsgegevens plaats. Het gaat hierbij om gegevens van burgers en (andere) organisaties, maar ook om gegevens van de eigen medewerkers. Vanuit de verantwoordelijkheid als overheidsorganisatie en als werkgever moet ook het ministerie zorgvuldig met persoonsgegevens omgaan.

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van wetten die het gebruik van persoonsgegevens regelen, zoals de AVG. Organisaties zoals VWS moeten ook een interne toezichthouder aanstellen: de Functionaris voor Gegevensbescherming (FG).

De FG houdt binnen het ministerie van VWS toezicht op de naleving van de AVG. Het toezicht van de FG is erop gericht om te verzekeren dat de minister voldoet aan zijn verplichtingen wat betreft het fundamentele recht op bescherming van persoonsgegevens. De beginselen van zorgvuldig gegevensgebruik vormen in de publieke sector voorwaarden voor rechtmatig overheidsoptreden en het vertrouwen van de burger in de overheid.

Voor u ligt het jaarverslag over de jaren 2019 en 2020 van de FG van het Ministerie van VWS.

Den Haag, april 2021

H. Westerling
Functionaris voor Gegevensbescherming VWS

1 Algemeen

1.1 Inleiding

De Functionaris voor Gegevensbescherming (FG) brengt tweejaarlijks verslag uit aan de Minister van VWS. Binnen de rijksoverheid is de minister verantwoordelijk voor de verwerking van persoonsgegevens. In termen van de AVG de verwerkingsverantwoordelijk. Voor u ligt het jaarverslag over de jaren 2019 en 2020.

1.2 Leeswijzer

Hoofdstuk 1 geeft een algemeen beeld. Hoofdstuk 2 gaat in op de werkzaamheden in 2019 en 2020. Tot slot geeft hoofdstuk 3 inzicht in belangrijke ontwikkelingen in het kader van privacy en de eventuele gevolgen voor VWS.

1.3 Persoonsgegevens en privacywetgeving

Bij het ministerie VWS verwerken we veel data. Het aanleggen, raadplegen, onderhouden en ter beschikking stellen van persoonsgegevens komt op veel plaatsen binnen VWS voor. Denk bijvoorbeeld aan het uitvoeren van diverse (gezondheid)onderzoeken, het bijhouden van diverse registers, het honoreren van subsidieaanvragen, het inspecteren van de gezondheidszorg, het in kaart brengen van het zorgveld, en het aannemen van nieuw personeel.

Privacywetgeving biedt een handvat om te kunnen beoordelen of bepaalde maatregelen en beleidskeuzes van VWS, waarbij het gebruik van persoons-gegevens aan de orde is, verantwoord zijn met het oog op de eisen van rechtmatigheid en behoorlijkheid. Ook is er sprake van een groei in privacyvraagstukken in relatie tot de coronacrisis[1]. De coronacrisis heeft gezorgd voor zowel meer verwerkingen van persoonsgegevens als meer verwerkingen van gevoelige en bijzondere persoonsgegevens binnen VWS.

1.4 Hoe is privacy in de organisatie belegd?

Binnen de rijksoverheid is de minister verantwoordelijk voor de verwerking van persoonsgegevens. De SG is eindverantwoordelijk voor de uitvoering en naleving van de AVG en andere relevante privacy wet- en regelgeving binnen VWS, met de pSG als gedelegeerd verantwoordelijke. De BRBV is het aangewezen gremium voor beleidsvorming en -vaststelling. Het lijnmanagement is verantwoordelijk voor verwerking van persoonsgegevens binnen de eigen directie of dienstonderdeel.

Bij VWS vindt de daadwerkelijke uitvoering van de AVG en relevante wetgeving plaats via DG-en en hun directeuren door proceseigenaren, afdelingshoofden en individuele medewerkers. Dit betekent dat een individuele beleidsmedewerker ervoor zorgt dat de activiteiten die hij/zij verricht ten behoeve van de beleidsonderwerpen die in zijn/haar portefeuille zitten, conform de AVG worden uitgevoerd. Via 'de lijn' leggen zij hierover verantwoording af aan hun DG-MT, opdat deze kan 'sturen' en in control is.

De concernonderdelen hebben elk tenminste één Privacy Officer (PO) die het lijnmanagement ondersteunt. Concernonderdelen zijn zelf verantwoordelijk voor het opbouwen van een goede structuur. Op de individuele staf- en beleidsdirecties van het kernministerie van VWS zijn de Privacy Contactpersonen (of Coördinatoren) het aanspreekpunt voor privacy vragen vanuit de directie.

[1] Uitbraak van het SARS-CoV-2, een virus dat kan leiden tot de ziekte COVID-19.

In 2019 is de Chief Privacy Officer aangesteld. De FG en de CPO werken sinds die tijd nauw samen om er zorg voor te dragen dat de gegevensverwerkingen door het ministerie aan de (U)AVG voldoen. De CPO ondersteunt met tweedelijns advies in specifieke gevallen en toetst de VWS-onderdelen op naleving. De FG houdt toezicht op de naleving van de AGV en adviseert op basis van DPIA's over voorgenomen verwerkingen. Het toezichtbereik van de FG strekt zich tot de beleidsdirecties en de concernonderdelen exclusief de ZBO's met een eigen rechtspersoon.

Aanvullend advies

Bij het kerndepartement dat in omvang is vergroot en waar fors meer privacyvraagstukken spelen merkt de FG op dat de privacyfuncties (privacy contactpersonen) aanscherping behoeven. Zodat vroegtijdig invulling gegeven kan worden aan het tijdig op kunnen nemen van privacyaspecten bij veranderingen van processen, voornemens van beleid- en wetswijzigingen en het verwerkingen van persoonsgegevens. En een rol bij de totstandkoming van een goede DPIA kan worden vervuld. Dit betekent dat de desbetreffende personen voldoende kennis en kunde ten aanzien van de AVG en het uitvoeren van DPIA's hebben. De FG raadt aan om de privacyfuncties te verstevigen.

Het RIVM is een organisatie van forse omvang, met zeer veel verwerkingen van persoonsgegevens. De FG merkt op dat hier nog veel sturing op nodig is. Hier speelt over het algemeen een governance aspect als wel zorgdragen dat de basis op orde is (bv. zorgdragen voor kwalitatieve DPIA's, het AVGregister). De vele persoonsgegevens die het RIVM verwerkt vraagt om een juiste inrichting van governance.

De FG adviseert daarnaast dat VWS meer gebruik maakt en kan maken van de *Flying Doctors* in het opzetten van DPIA's. De *Flying Doctors* is een pool van medewerkers die opgeleid zijn om te begeleiden bij het uitvoeren van een DPIA. Gesignaleerd wordt dat de organisatie worstelt met het opstellen van DPIA's en er meer gebruik gemaakt kan worden van de kennis die al aanwezig is in de organisatie. Hiervoor is het noodzakelijk dat in de *Flying Doctors* geïnvesteerd wordt door meer tijd en capaciteit beschikbaar te maken voor ondersteuning.

2 Werkzaamheden 2019 en 2020

De FG treedt op als toezichthouder, geeft adviezen en doet aanbevelingen om te zorgen dat de organisatie zo veel mogelijk in lijn met de AVG handelt.

2.1 Coronacrisis

De jaren 2017 en 2018 waren belangrijke jaren in de aanloop naar het op 25 mei 2018 van toepassing komen van de AVG. Het jaar 2019 betrof met name het bestendigen van de AVG in de organisatie. De coronacrisis heeft ertoe geleid dat vanaf maart 2020 de werkzaamheden van de FG grotendeels gerelateerd waren aan de privacyvraagstukken die opkwamen in de monitoring en bestrijding van COVID-19. Dit betrof vraagstukken zoals de ontwikkeling van CoronaMelder, het Corona Dashboard en het Vaccinatieregister (CIMS).

2.2 Gegevensbeschermingseffectbeoordeling (GEB-PIA, hierna DPIA)

De AVG legt verantwoordelijkheid bij de organisatie om aan te tonen dat aan de privacyregels is voldaan. Deze verantwoordingsplicht (accountability) houdt in dat de organisatie moet kunnen aantonen dat de verwerkingen aan de regels van de (U)AVG voldoen. Het uitvoeren van een data privacy impact assessment (DPIA) voor gegevensverwerkingen met een hoog privacyrisico is een verplichte maatregel voor de verantwoordingsplicht van een organisatie. Door te voldoen aan haar verantwoordingsplicht (accountability) levert de organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.

Een DPIA is een instrument om van voorgenomen regelgeving of projecten waarbij persoonsgegevens worden verwerkt, de impact voor de privacy van de betrokkenen in kaart te brengen en te beoordelen. Op basis hiervan worden maatregelen getroffen om deze effecten voor betrokkenen te voorkomen of verkleinen.

Waar in 2017 en 2018 de focus lag op de implementatie van de AVG, is de organisatie volwassener geworden en zijn er in 2019 en 2020 beduidend meer DPIA's plaatsgevonden, een verdubbeling in aantal. Toezicht door middel van beoordeling en uitgebrachte FG-adviezen op DPIA's stond daarom centraal in de werkzaamheden van de FG in de jaren 2019 en 2020. Naast dat de DPIA een belangrijk onderdeel van haar verantwoordingsplicht voor de organisatie betreft dient de DPIA ook als een instrument voor de FG om toezicht op de werkwijze, de omgang met en bescherming van persoonsgegevens door de organisatie te kunnen uitvoeren.

De FG adviseert bij een DPIA, zowel over de inhoudelijke beoordeling als de naleving van de voorgenomen beheersmaatregelen en schakelt met de CIO in geval het een DPIA op een ICT-systeem is.

In 2020 zijn 44 DPIAs (2019: 30x) beoordeeld op kwaliteit en de beheersing van de privacyrisico's voor de betrokkenen. Dit betrof zowel in 2019 als in het jaar 2020 10 DPIA's ten behoeve van wetsvoorstellen (wetsvoorstellen, amvb's en ministeriele regelingen). In 2020 betroffen de DPIA's met name gegevensverwerkingen coronacrisis gerelateerd. Zoals de CoronaMelder, het Vaccinatieregister en verschillende onderzoeken in het kader van COVID-19 bij het RIVM.

Algemeen kan gesteld worden dat een goede begeleiding met deskundigheid op het uitvoeren van een DPIA essentieel is. De kwaliteit komt dan beduidend ten goede. De privacyrisico's voor de rechten en vrijheden van betrokkenen komen beter in zicht. De vragenlijst die wordt gehanteerd om een DPIA af te nemen, dient te worden beschouwd als een beginpunt voor een belangenafweging, waarbij de

verantwoordelijke zich de vraag moet stellen: Wat wil ik bereiken? Is het noodzakelijk hiervoor persoonsgegevens te verwerken en kan ik mijn doel niet op een andere manier bereiken? Is er een grondslag voor het verwerken van de voorgenomen gegevensverwerkingen aanwezig? Zijn de juiste persoonsgegevens geselecteerd? En, als al deze vragen bevestigend zijn beantwoord: welke beveiligingsmaatregelen moet ik treffen om de persoonsgegevens te beschermen?

Het is belangrijk dat het uitvoeren van een DPIA vooral wordt gedaan om goed zicht te krijgen de voornaamste (rest)risico's, zodat de verwerkingsverantwoordelijke deze kan afwegen, waar mogelijk adresseren en eventueel accepteren.

Een goede begeleiding bij het uitvoeren van een DPIA is met name van belang om scherpte te houden op de verwerkingsketen. Wanneer een verwerking niet op zichzelf staat, maar deel uitmaakt van een keten, kan de vraag naar het doel van de verwerking niet los gezien worden van het doel van de keten. In zo'n geval is het essentieel in te gaan op de vraag hoe de verwerking zich verhoudt tot het hogere doel. Draagt het hieraan bij? Is dit mogelijk door minder persoonsgegevens te verwerken? Bij een verwerking die deel uitmaakt van een verwerkingsketen, dient extra aandacht te worden geschonken aan de verantwoordelijkheidsverdeling tussen de verschillende proceseigenaren in de keten. In het bijzonder moet men alert zijn op de vraag of er verwerkersovereenkomsten moeten worden gesloten.

Aanvullend advies FG

DPIA's dienen als hulpmiddel voor de organisatie, maar worden vaak gezien als verplichte stap in een proces. Het blijft aanbevelingswaardig om het uitvoeren van een DPIA zo vroeg mogelijk in het proces te laten plaatsvinden, zodat de DPIA een echte meerwaarde kan geven op de vervolgstappen en het ontwerp binnen een project, programma of wetsvoorstel.

Het valt de FG op dat het identificeren van potentiële privacy risico's als een lastige opgave wordt beschouwd. Regelmatig richt men zich alleen op de informatiebeveiligingsrisico's zonder stil te staan bij de privacy risico's voor de betrokkenen. De FG adviseert dan ook om bij de DPIA's goed na te denken over wat de privacy risico's zijn in plaats van alleen te richten op informatiebeveiligingsrisico's. Een privacy risico is een kans op het optreden van een negatief gevolg voor de rechten en vrijheden van de betrokkenen als gevolg van de verwerking van persoonsgegevens. Bij de rechten en vrijheden van de betrokkenen moet in eerste instantie aan het recht op privacy worden gedacht, maar ook aan andere fundamentele rechten en vrijheden, zoals de vrijheid van meningsuiting, de vrijheid van godsdienst en het verbod op discriminatie. Het voordoen van een (hypothetische)situatie kan leiden tot lichamelijke, materiële en immateriële schade voor de betrokkene. Hierbij kan gedacht worden aan de situaties waar de gegevensverwerking kan leiden tot discriminatie, stigmatisering, uitsluiting, blootstelling aan identiteitsdiefstal of –fraude, reputatie- en of andere zins relationele schade, verlies van vertrouwen van door het beroepsgeheim beschermde persoonsgegevens. Zoals in hoofdstuk 1 al aangegeven adviseert de FG om de PIA deskundigheid van de zogeheten '*Flying Doctors*' van directie Informatiebeleid/CIO meer in positie te brengen door deze pool meer bekendheid te geven. Zodat een goede begeleiding met deskundigheid bij het uitvoeren van een DPIA ingezet kan worden.

Vervolg aanvullend advies FG
Er is een trend zichtbaar dat vaker voorafgaand aan een wetsvoorstel of besluit een pilot, experiment uitgevoerd wordt. Om inzicht te krijgen in de haalbaarheid, opzet en verloop van een beleidsvoornemen is dit een logische insteek. Echter het is hierbij wel van belang om alert te zijn op wat de voorgenomen verwerking betekent bij een landelijke uitrol of *live gang*. De afwegingen ten aanzien van de privacy risico's voor de rechten en vrijheden van de betrokkenen kunnen verschillen tussen het uitvoeren van een pilot/experiment en een landelijke uitrol. Zo kan de populatie van betrokkenen vele malen groter worden, andere uitvoeringsrisico's aan de orde zijn door andere en meer betrokken partijen bij een landelijke uitrol. De FG adviseert om al bij de uitvoering van de DPIA voor een pilot/experiment rekening te houden met de privacy risico's ten aanzien van een landelijke uitrol.

2.3 Adviezen door de FG

In de functie van toezichthouder kan de FG de organisatie gevraagd en ongevraagd adviseren. Afgelopen jaren is gebleken dat vanuit de organisatie ook behoefte bestaat aan deskundig, onafhankelijk advies inzake de AVG. Het laat onverlet dat het lijnmanagement verantwoordelijk blijft voor de juiste naleving van de privacywetgeving.

Er zijn in 2019 en 2020 door de FG tientallen adviezen (2020: 33, 2019: 15) gegeven. De adviezen waren zeer divers van soms zeer uitvoerend van karakter, zoals het beoordelen van verwerkingsovereenkomsten tot aan meer procesmatig in het kader van de coronacrisis. In het licht van de coronacrisis komen enkele elementen vaker terug zoals de aanwezigheid en verkrijgen van een wettelijke grondslag, scherpte in de rollen ten aanzien van verwerkingsverantwoordelijke versus verwerker en hiermee eigenaarschapsbepalingen, als wel de bewustzijn van dataminimalisatie.

De rode draad bij de adviezen betreft vooral het scherp krijgen van welke persoonsgegevens verwerkt worden en hulp bij de afweging van het nut en noodzaak van het gebruik van dergelijke gegevens. Als wel inzichtelijk maken van de privacy risico's. Door enkel die persoonsgegevens te verwerken die daadwerkelijk nodig zijn, worden de privacy risico's verkleind.

2.4 Meldplicht datalekken

Het acteren op (mogelijk) datalekken[2] en het onderzoeken van signalen is in eerste instantie een lijnverantwoordelijkheid. De FG heeft als taak toezicht te houden of de juiste handelingen als adequaat reageren, het nemen van de juiste corrigerende maatregelen en het maken van een juiste afweging door de organisatie heeft plaatsgevonden. Het ondersteunen van het lijnmanagement bij het afhandelen datalekken is een taak van de Privacy Officer met als tweede lijn de Chief Privacy Officer. Datalekken van grotere omvang en/of impact worden daarnaast direct gemeld bij de FG. De FG heeft inzage in het datalekkenregister. Op 26 september 2019 is de eerste versie van het Draaiboek Informatie Incidenten en datalekken VWS vastgesteld in het Integraal Beveiligingsoverleg Concern (IBC).

In 2019 zijn **88** datalekken en in 2020 **50** datalekken in het centrale datalekregister van VWS opgenomen. Het valt op dat opnieuw, vergelijkbaar met 2017/2018, het verlies van poststukken een groot aandeel in de datalekmeldingen betreft. Ook daar waar het privacygevoelige gegevens betreft zijn poststukken uit het zicht geraakt, dan wel verloren gegaan.

[2] De verordening spreekt van een inbreuk in verband met persoonsgegevens.

De daling in aantal vindt zijn oorzaak in het feit dat de datalekprocedure dusdanig aangepast is dat enkel de aan de AP meldingswaardige datalekken vanaf 2020 in het centrale datalekregister opgenomen staan. Naast het centrale datalekregister hanteren de afzonderlijke dienstonderdelen een eigen decentraal datalekregister waarin alle (vermoedelijke) datalekken bij het desbetreffende organisatieonderdeel opgenomen staan. Verder kan gemeld worden dat in 2020 meer duidelijkheid is ontstaan over wat wel en niet te melden bij de AP. Zo heeft de AP helderheid gegeven over het begrip betrouwbare personen, waarbij indien van toepassing een melding aan de AP niet noodzakelijk is. Als wel hoe om te gaan met bulkmeldingen.

In 2020 is de FG betrokken geweest bij 2 grote datalekken; te weten het donorregister en Infectieziekteradar. De FG is in 2019 bij 15 datalekken actief betrokken geweest en in 2020 bij 7 datalekken.

In onderstaande tabel is een overzicht naar verdeling van het type datalek weergegeven.

	Types	2019	2020
1	Een poststuk met persoonsgegevens komt niet aan bij de ontvanger of komt geopend terug	39 %	50 %
2	Een dossier of documenten zijn foutief samengesteld (niet geanonimiseerd, foutieve bijlagen etc.)	19 %	30 %
3	Een email met persoonsgegevens komt bij de verkeerde ontvanger terecht.	16 %	8 %
4	Onjuiste autorisaties, IT-instellingen	6 %	0 %
5	Verlies van gegevensdragers, dossiers	9 %	2 %
6	Overig divers	9 %	5 %

Tabel 1: Verdeling datalekken 2019 en 2020

Aanvullend advies FG
Het blijft aanbevelingswaardig om waar mogelijk altijd gebruik te maken van gepseudonimiseerde gegevens en bij voorkeur van geanonimiseerde gegevens. Naast de verplichtingen om hiermee te voldoen aan de privacyprincipes van de AVG draagt het aanzienlijk bij aan het voorkomen van een mogelijk datalek. Waardoor de mogelijke impact voor de betrokkenen (datgene waar het uiteindelijk om gaat) verkleind.

2.5 FG contacten met de burger

Zoals de AVG voorschrijft kunnen betrokkenen met de FG contact opnemen over alle aangelegenheden die verband houden met de verwerking van hun gegevens en met de uitoefening van hun rechten.

De FG is bereikbaar voor betrokkenen door middel van de FG postbus. De vragen of klachten die binnenkomen via de FG postbus zijn geregeld uitvoeringsvraagstukken. Deze signalen worden doorgezet binnen het departement.

In 2019 hebben zich 22 burgercontacten plaats gevonden, en in 2020 17 burgercontactmomenten. De contacten betroffen met name burgers met vragen over de verwerking van zijn/haar gegevens in het kader van het Donorregister en medio 2020 tot heden COVID-19 gerelateerde vragen. Dit laatste met name vragen over gegevensverwerkingen ten aanzien van het vaccinatieregister bij het RIVM. Als wel burgercontacten met een vraag, signaal ten aanzien van gegevensverwerking dat betrekking had op het zorgveld, waaronder GGD-en en zorgverleners, welke

buiten het toezichtbereik van de FG valt. Ook zijn er enkele casussen met specifieke burgercontacten geweest waarbij men klachten ten aanzien van bijvoorbeeld het tuchtcollege als het CIBG heeft. Over het algemeen betreft dit burgers die het niet eens zijn met een genomen beslissingen en via de FG zijn of haar grieven aangeeft.

2.6 FG contacten met de AP

De FG treedt op als intermediair tussen VWS en de AP in voorkomende kwesties. In 2020 heeft de FG beduidend meer contact met de AP gehad. Dit betrof in totaal 15 contactaangelegenheden ten aanzien van het volgende zaken:

- Vraagstukken die de AP had betreffende de verwerking van persoonsgegevens COVID-19 gerelateerd, zoals CoronaDashboard, CoronaMelder, testen van zorgpersoneel etc.;
- vraagstukken waarbij de AP vanuit de burger vragen en signalen heeft ontvangen;

Daarnaast heeft contact plaatsgevonden ten aanzien van de informatieverzoeken van de AP ten aanzien van de twee grote datalekken (donorregister-CIBG en infectieziekteradar-RIVM) waar het ministerie mee te maken heeft gehad.

2.7 Voorlichting

Het bewust zijn van een zorgvuldige omgang met persoonsgegevens, kennis van de *do's* en *don'ts* bij verwerkingen van persoonsgegevens en kennis van de wetgeving is een belangrijke basis in het zorgvuldig omgaan met deze gegevens.

Voorlichtingsactiviteiten hebben zich vooral in 2019 voorgedaan. Zoals een bijdrage aan de PIA training van de *Flying Doctors*, het bewustwordingsfilmpje van de RTE, presentatie in het juristennetwerk (over het beoordelen van DPIA's door de FG). Als wel een presentatie in het kader van de week van de privacy bij het CIBG. Door de coronacrisis en de vele privacyvraagstukken die hieruit voortvloeien is actieve voorlichting in 2020 beperkt geweest. Wel is de FG is aanwezig geweest bij verschillende DPIA sessies. Dit heeft met name tot doel voorlichting om een kwalitatief hoogwaardige DPIA tot stand te laten komen als wel om zorg te dragen dat de juiste diepgang op het inzichtelijk maken van de privacyrisico's tot stand komt.

2.8 Overleggremia

2.8.1 Privacykring

Dit platform is door de FG van VWS in 2017 vormgegeven. Vanwege de scheiding tussen uitvoerende en toezichthoudende taken is het voorzitterschap van dit overleg in 2019 overgedragen aan de Chief Privacy Officer. De Privacykring komt elke maand bij elkaar en bespreekt de stand van zaken op het privacydomein en nieuwe ontwikkelingen en producten. De leden zijn Privacy Officers van de concernonderdelen. De FG sluit aan als gast.

2.8.2 CISO-overleg (IBX)

Het centrale en decentrale verantwoordelijkheidsniveau zijn qua informatieveiligheid verbonden via het CISO-overleg van VWS; zijnde het IB-expertoverleg (IBX). In dit gremium zitten de CISO VWS en de (C)ISO's van de afzonderlijke VWS-onderdelen. De FG neemt als gast deel aan het IBX aangezien informatieveiligheid een belangrijke pijler bij het beschermen van persoonsgegevens is.

2.8.3 Rijksplatform van Privacyfunctionarissen (RPFG)

Hierin zijn de departementale FG's verenigd. Dit overleg is uitdrukkelijk een informeel overleg en is bedoeld om ervaringen en best practices te delen. In deze gremia werden thema's behandeld in het kader van afstemming, kennis-overdracht, en het oppakken en behandelen van gemeenschappelijke kwesties.

Daarnaast functioneert het RPFG als portaal voor FG advies voor voorgenomen gegevensverwerkingen ten aanzien van rijksbrede informatievoorzieningen. Hierbij wordt de PAR-procedure van het ministerie van BZK gevolgd.

2.8.4 *Informerend Overleg Beroepsgeheim en Privacy (IOBP)*
Gemiddeld eens per twee maanden overlegt binnen VWS het Informerend Overleg Beroepsgeheim en Privacy (IOBP): een wederzijds informerend concernbreed overleg om afstemming en coördinatie van aspecten over het medisch beroepsgeheim en privacy te bevorderen. Het IOBP is uitdrukkelijk geen besluitvormend gremium en het voorzitterschap en secretariaat zijn belegd bij WJZ. De FG neemt deel aan het IOBP.

2.8.5 *Functionaris voor Gegevensbescherming Overleg VWS (FGO)*
Sinds 2019 is op initiatief van de FG VWS een regulier FG overleg opgestart met de Functionarissen voor Gegevensbescherming van de publiekrechtelijke ZBO's binnen het VWS concern. Gemiddeld elk kwartaal vindt er een overleg plaats met de FG's van de publiekrechtelijke ZBO's VWS. Dit zijn de FG's van het CAK, CIZ, ZiNL, NZA, ZonMW en de Dopingautoriteit. De FG is voorzitter van dit overleg. Dit overleg is uitdrukkelijk een informeel overleg en is bedoeld om ervaringen en best practices te delen.

3 Ontwikkelingen en vooruitblik

3.1 Ontwikkelingen

Door nieuwe technologie kan VWS makkelijker veel verschillende soorten gegevens verzamelen en aan elkaar koppelen en gegevens uitwisselen. Ook wordt meer gebruik gemaakt van grote hoeveelheden van informatie om bepaalde verbanden te vinden (big data). Het risico hierbij is dat de organisatie het zicht verlies op welke gegevens zij allemaal verwerken en waarvoor zij dat doet.

Telkens zullen bij deze ontwikkelingen de eisen van zorgvuldigheid en privacy meegenomen moeten worden. Binnen dat spanningsveld tussen efficiency en zorgvuldigheid moet een organisatie opereren. Een goede toepassing van beginselen zoals die van doelbinding, proportionaliteit en subsidiariteit speelt een belangrijke rol. Bewustwording en toezicht draagt daaraan bij. Behalve dat er oog moet zijn voor de (primaire) voorwaarden waaronder het gebruik van persoonsgegevens mag plaatsvinden, dienen ook de overige verplichtingen uit de (U)AVG niet uit het oog worden verloren: de mogelijkheid tot uitoefening van rechten door betrokkenen, de zorg voor de kwaliteit van gegevens, de naleving van informatieverplichtingen richting de betrokkenen, naleving van bewaartermijnen en de beveiliging van de persoonsgegevens.

3.2 Privacy by Design

Privacy by design betekent dat in een vroeg stadium al aandacht is voor zorgvuldige omgang met persoonsgegevens. Wanneer de basishouding privacy by design ademt en dit de hoogste prioriteit krijgt in de opzet voor het behalen van de doelen, voorkomt dit dat later in het traject er vele maatregelen getroffen dienen te worden op het vlak van privacy en informatiebeveiliging die het traject vertragen en compliceren. De FG merkt op dat bij verwerkingen waar privacy by design als grondhouding in de aanpak is ingebed, zoals bijvoorbeeld CoronaMelder beduidend minder privacy issues aan de orde zijn.

Aanvullend advies FG

Zoals ook in het voorgaande jaarverslag aangegeven is het aan te bevelen om te blijven inzetten op het in een vroeg stadium toepassen van privacy by design bij projecten, het formeren van beleid en opzetten van IT-systemen. Met privacy by design wordt bedoeld, dat in het ontwerp van een verwerking al rekening wordt gehouden met de privacybescherming, bijvoorbeeld door de persoonsgegevens te pseudonimiseren bij de bron. Maar boven al om het construct (=de wijze waarop) en de zogeheten data infrastructuur zodanig in te richten dat dataminimalisatie ten volle wordt uitgevoerd. En goed stil te staan op welke minder privacy ingrijpende manier het ook mogelijk is. Dit betreft een andere manier van denken, daar waar we geneigd zijn om de mogelijke kwetsbaarheden met beveiligingsmaatregelen aan te pakken, denk aan encryptie, logging en monitoring. Deze maatregelen wegen niet op tegen het in de basis van het ontwerp baseren op privacy by design. Het valt op dat privacy by design ten volle tot uiting komt als de proces/product requirements privacy by design als uitgangspunt heeft en het een doel op zich betreft.

3.3 Vooruitblik

Het adviseren op DPIA's stond in de jaren 2019 en 2020 centraal. Naar verwachting zal dit, gezien het feit dat Nederland ten schrijven van dit jaarverslag zich nog in de coronacrisis bevindt, ook voor 2021 zich voortzetten. Een crisis waarbij de verspreiding van SARS-CoV-2 wordt beteugeld door diverse maatregelen. Daar waar bewegingsvrijheid worden beperkt door een lockdown, ontstaat ook de behoefte om op een gecontroleerde manier de samenleving weer te openen. Met initiatieven waarbij al dan niet verwerkingen van persoonsgegevens aan de orde komen, denk aan testbewijzen, vaccinatiebewijzen en nadere onderzoeken door het RIVM.

Aanvullend advies FG

Naast het voortzetten van periodieke voortgangsrapportage in de vorm van een selfassessments en het uitvoeren van DPIA's is het ook aan te bevelen om aandacht en prioriteit te blijven geven aan het up tot date houden van het AVGregister. Het AVGregister is een belangrijk element in het aantoonbaar maken van het voldoen aan de AVG door de organisatie.

Bijlage: Afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BRBV	Bestuursraad bedrijfsvoering
CIO	Chief Information Officer
CPO	Chief Privacy Officer
DPIA	Data Privacy Impact assessement
FG	Functionaris voor Gegevensbescherming
GEB-PIA	Gegevenseffectbeoordeling - Privacy Impact assessment
IBX	Informatiebeveiliging Expertgroep
IOBP	Informerend Overleg Beroepsgeheim en Privacy
PA	Privacy Adviseur
PC	Privacy Contactpersoon
PO	Privacy Officer
pSG	Plaatsvervangend Secretarisgeneraal
RPFG	Rijks Platform voor Functionarissen gegevensbescherming
SG	Secretaris-generaal
VWS	Ministerie van Volksgezondheid, Welzijn en Sport
WJZ	Directie Wetgeving en Juridische Zaken
ZBO	Zelfstandig Bestuursorgaan