Regio Gooi en Vechtstreek

MEMO

Verslag Functionaris Gegevensbescherming over periode juli 2021 - juni 2022

Algemeen	
Aan	CMT, DB, AB
Van	Anne Cnossen
Datum	15 juli 2022
Verspreiden	Nee
Kenmerk	22.0003234

Samenvatting

Dit is het vierde verslag van de Functionaris Gegevensbescherming (FG) aan het Dagelijks Bestuur. Het verslag beslaat de periode juli 2021 tot en met juni 2022.
Belangrijke gebeurtenissen op het gebied van privacy in het afgelopen verslagjaar betreffen:
- de verbeteringen van de landelijk en regionale inrichting van de GGD-processen als gevolg van het onderzoek van de Autoriteit Persoonsgegevens (AP)
- het overdragen van taken (met bijbehorende dossieroverdracht) aan Amsterdam voor de Weesper inwoners
- de start van het werken met een DPIA (privacy risicoanalyse)-kalender binnen de Regio
- de aanval met phishing mails waarmee een hacker geprobeerd heeft aan wachtwoorden te komen.
- de implementatie van de Wet politiegegevens (Wpg) die van toepassing is op boa's bij GAD en RBL
- de intensivering van de samenwerking tussen de FG en FG's van regiogemeente ten aanzien van advisering
- de start van de uitrol van Office 365

Het verslagjaar stond het eerste half jaar (tot en met december 2021) op het gebied van privacy nog steeds grotendeels in het teken van corona. Vanaf januari was er wat meer ruimte voor de focus op de andere organisatieonderdelen van de Regio.
Er is een start gemaakt met de uitrol van specifiekere privacyverklaringen voor de websites van de organisatieonderdelen. En er is hard gewerkt om de aanbevelingen uit de nulmeting Wpg op te volgen.
De trend van het vorig verslagjaar waarin veel meer interne meldingen van mogelijke datalekken zijn gedaan dan voorgaande jaren is dit verslagjaar voortgezet. Zoals elk jaar is er een evaluatie uitgevoerd op de gemelde datalekken en op de procedure tot afhandeling van deze meldingen.
Ook zijn weer enkele risicoanalyses uitgevoerd op verwerkingen van persoonsgegevens met een hoog risico. Vanaf nu werken we daarvoor met een DPIA-kalender die aan het begin van een kalenderjaar aangeeft welke DPIA's er dat jaar zullen worden uitgevoerd.

Komend jaar is het oppakken van zaken waarvoor in afgelopen jaar te weinig tijd beschikbaar was van belang. Het gaat om het verder uitwerken van het privacybeleid door de organisatieonderdelen. Tegelijkertijd moet ook het register van gegevensverwerkingen op één plek (het nieuwe DMS Decos) beschikbaar komen zodat aandachtsfunctionarissen privacy en FG hier samen aan kunnen werken. Het bewustwordingstraject moet een verdere boost krijgen door de uitrol van de e-learning gereed te maken (enkele organisatieonderdelen zijn nog niet aan de beurt geweest). De verdeling van verantwoordelijkheden voor de AVG tussen Regio en regiogemeenten is niet altijd duidelijk en moet

beter geduid worden in de gemeenschappelijke regeling. Verwerkersovereenkomsten moeten beter worden ingevuld, hiertoe zal een nieuw sjabloon beschikbaar komen.
Het verslag bevat ten slotte wederom een aanbeveling over structurele uitbreiding van de personele bezetting op het gebied van privacy om de meer praktische, proactieve privacywerkzaamheden beter op de rit te krijgen.

Inhoudsopgave

1 Inleiding

Dit is het vierde verslag van de Functionaris Gegevensbescherming (hierna: FG) aan het Dagelijks Bestuur (hierna: DB). In de Algemene Verordening Gegevensbescherming (hierna: AVG) en de Wet politiegegevens (hierna: Wpg) is geregeld dat de FG verslag uitbrengt over zijn werkzaamheden, bevindingen en aanbevelingen aan de verwerkingsverantwoordelijke, bij de Regio het DB. Om deze reden wordt dit verslag aangeboden aan het CMT, het DB en ook aan het Algemeen Bestuur als controlerend orgaan. Elk jaar in juli verschijnt een dergelijk verslag.
In dit verslag staat aan de hand van belangrijke privacythema's beschreven welke acties en maatregelen de Regio in het afgelopen verslagjaar (van juli 2021 tot en met juni 2022) heeft genomen om de doelstellingen en beginselen uit de AVG te behalen en te waarborgen. Ten opzichte van het verslag over de vorige periode is er een thema toegevoegd, namelijk de Wet politiegegevens. In 2021 werd voor de Regio duidelijk dat voor de Wpg ook nog veel ingeregeld moest worden. Omdat de Wpg ook een jaarlijks verslag van de FG voorschrijft, is een apart hoofdstukje in dit verslag daarvoor op zijn plaats. In het verslag wordt vaak gerefereerd aan de AVG omdat die voor het overgrote deel van de Regio leidend is. Vanwege de grote overlap tussen AVG en Wpg is het zo dat de Regio met het voldoen aan de AVG ook Wpg-compliant is. Als er in dit verslag iets wordt gezegd over een verplichting die exclusief in de Wpg staat of in de Wpg anders is geregeld, dan wordt de Wpg wel expliciet vermeld. Waar van toepassing wordt aangegeven welke zaken al op de planning staan voor komend verslagjaar. Ook bevat dit document de bevindingen van de FG en aandachtspunten voor het komende jaar. Adequaat omgaan met persoonsgegevens is een blijvend proces en zal dan ook aandacht blijven vergen van zowel bestuur, management als medewerkers. Ten slotte wordt een aanbeveling gedaan waarmee de implementatie en borging kan worden versterkt.

2 Organisatorische inbedding

Context
Het DB is verantwoordelijk voor goede gegevensbescherming binnen de Regio. Managers en medewerkers hebben een hiervan afgeleide verantwoordelijkheid. De FG houdt toezicht op een goede omgang met persoonsgegevens volgens de AVG en Wpg.
Alle managers hebben één of meerdere aandachtsfunctionarissen privacy benoemd om hen te ondersteunen in hun privacytaken. De aandachtsfunctionaris is het eerste aanspreekpunt voor privacy voor zijn/haar eigen organisatieonderdeel en voor de FG. Zij signaleren wijzigingen in de verwerkingen van persoonsgegevens en coördineren voor hun organisatieonderdeel de afhandeling van de organisatiebrede verzoeken (zoals verzoeken om inzage) die inwoners en medewerkers vanuit de AVG en Wpg bij de Regio kunnen indienen. Een aantal keren per jaar spreekt de FG afzonderlijk met de verschillende aandachtsfunctionarissen privacy. Daarnaast is het de bedoeling eens per jaar een gesprek met de RVE/organisatieonderdeel-managers te plannen.

Voortgang in verslagjaar
De FG en plaatsvervangend FG waren tot dit jaar enkel als toezichthouder voor de AVG aangewezen maar zijn dat nu ook voor de Wpg.
Inmiddels is de manager WSP zelf de aandachtsfunctionaris privacy voor zijn organisatieonderdeel. De Adviseur Informatie vervult deze rol nu voor Bedrijfsvoering. Daarnaast is afgesproken dat FG en juridisch adviseurs vanaf nu weer vaste aanspreekpunten krijgen bij Sturing/Sociaal Domein zodat ook in het werk van Sturing eerder rekening wordt gehouden met aandachtspunten op algemeen juridisch en gegevensbeschermingsgebied.

Bij de afdeling Toezicht en Handhaving van de GAD is een bevoegd functionaris[1] opgeleid en aangesteld die een poortwachtersfunctie vervult voor de verstrekkingen naar buiten de Regio van politiegegevens in de grotere opsporingsdossiers.
Afgelopen jaar heeft de FG met alle aandachtsfunctionarissen gesproken. De gesprekken met de managers zijn niet allemaal consequent gevoerd.

Acties komende jaar
Het verder intensiveren van de één op één gesprekken tussen FG en aandachtsfunctionarissen privacy en RVE/organisatieonderdeel-managers is komend jaar weer van belang.

3 Kennis en kunde privacy

Context
Het is van belang dat de diverse functionarissen die zich met privacyzaken bezig houden kennis en kunde op peil brengen en houden.

Voortgang in verslagjaar
Uit het maandelijks samenkomende netwerk van FG's en Privacy Officers van de regiogemeenten en de FG van de Regio komen nuttige ervaringen en best practices naar voren die ook door de Regio worden benut.
Diverse personen die zijn betrokken bij de Wpg-audits hebben zich met een cursus verder bekwaamd in de Wpg. En in GoodHabitz is een leuke cursus privacy beschikbaar die bij de aandachtsfunctionarissen privacy onder de aandacht is gebracht.

4 Advisering, informatieverstrekking en voorlichting

Context
Formele adviezen aan verwerkingsverantwoordelijke (vaak RVE-manager/CMT) worden gegeven wanneer er risico's voor de privacy van inwoners/medewerkers bestaan of als er onduidelijkheid bestaat over de uitvoering van een bepaalde gegevensverwerking.
Van de formele adviezen van de FG kan de verwerkingsverantwoordelijke enkel gemotiveerd afwijken.

Voortgang in verslagjaar
De FG heeft een aantal formele adviezen gegeven waarop de verwerkingsverantwoordelijke heeft gereageerd. Een aantal adviezen is overgenomen en van een aantal is gemotiveerd afgeweken. Zie **bijlage 1** voor meer informatie over deze formele adviezen. Een aantal van de adviezen had te maken met de overdracht van taken met bijbehorende dossiers naar Amsterdam. In het kader van de bestrijding van corona is er, net als voorgaande jaren, intensief contact tussen FG en Directeur Publieke Gezondheid, waarbij enkele formele adviezen door de FG zijn gegeven met name over het al dan niet meegaan in landelijk ontwikkelde systemen en processen. Deze adviezen zijn niet in bijlage 1 opgenomen.
Daarnaast is veelvuldig een beroep op de juridisch adviseurs en FG gedaan voor (informeel) advies bij alle aangelegenheden waarbij medewerkers binnen de organisatie te maken hadden met verwerking van persoonsgegevens. Ten slotte werd vaak advies verstrekt bij vragen over het AVG-proof inrichten van verschillende afdelingen en werkprocessen.

[1] Deze functionaris is verplicht voor bepaalde zwaardere Wpg-verwerkingen en beslist bijvoorbeeld wie er toegang mag hebben tot politiegegevens en of ze verstrekt kunnen worden aan een samenwerkingspartner.

5 Toezicht op toepassing en naleving AVG

Context
De FG houdt toezicht op een goede omgang met persoonsgegevens volgens de AVG en het privacybeleid.

Voortgang in verslagjaar
Toezicht is het afgelopen jaar vooral reactief uitgeoefend als daarvoor een trigger was. Triggers waren met name de geformuleerde maatregelen in de nasleep van datalekken en uitspraken van de AP. Een belangrijke trigger voor toezicht op de processen rondom de coronabestrijding bij de GGD was het onderzoek van de Autoriteit Persoonsgegevens naar aanleiding van de datadiefstal bij GGD GHOR Nederland die in januari 2021 aan het licht kwam. Ook zijn er weer gesprekken geweest met de aandachtsfunctionarissen waarin door de FG adviezen ter verbetering zijn gegeven.

6 Wet politiegegevens

Context
Als boa's bezig zijn met de opsporing en vervolging van strafbare feiten verwerken zij politiegegevens en is de Wet politiegegevens (Wpg) van toepassing. Een belangrijk verschil tussen AVG en Wpg is dat de laatste een verplichte jaarlijkse interne audit en een vierjaarlijkse externe audit kent.

Voortgang in verslagjaar
Eind 2021 heeft de Regio een nulmeting/interne audit Wpg laten uitvoeren. Hieruit kwamen de nodige verbeterpunten naar voren. Dit was niet erg verrassend gezien het feit dat de Regio pas in 2021 zich ervan bewust is geworden dat ze daar van alles voor moet organiseren. De Regio is in 2022 aan de slag gegaan met het verder implementeren van de Wpg bij de GAD en RBL (waar de boa's werken die onder de Wpg vallen), op basis van de aandachtspunten uit de interne audit. Het betreft nu nog voornamelijk het op orde brengen van de processen. Tevens is een start gemaakt met de voorbereiding van de externe audit Wpg over de periode tot en met 2021 die eind 2022 zal plaatsvinden.
In het kader van de implementatie heeft de FG vooral de rol van kwartiermaker en adviseur vervuld.

Acties komende jaar
Voor de Wpg moet eerst nog worden verdergegaan met het inrichten van procedures, vervolgd met het werken volgens deze procedures, de interne audit 2022 in het najaar, de externe audit over 2021 eind oktober en het verbeterplan n.a.v. de externe audit. Omdat de externe audit over 2021 gaat, het jaar waarin de Regio nog amper aan de Wpg voldeed, zullen een aantal aanbevelingen uit de externe audit inmiddels als zijn opgepakt/gerealiseerd. In het komende jaar zal de FG ook zijn toezichthoudende taak ten aanzien van politiegegevens gaan uitoefenen.

7 Bewustwording

Context
Bewustwording bij bestuur, management en medewerkers over het belang van privacy en de regels hierover is een belangrijke voorwaarde om duurzaam aan de AVG te voldoen.

Voortgang in verslagjaar
De uitrol van de e-learning privacy met als doel het vergroten van de digitale weerbaarheid van de Regio en haar medewerkers is afgelopen jaar nog niet volledig afgerond.
Vragen over privacy en afwikkeling van datalekken worden aangegrepen om privacybewustwording bij management en medewerkers te vergroten. De gesprekken met aandachtsfunctionaris privacy en

manager worden gebruikt om daar o.a. aandacht te vragen voor het belang van blijvend privacybewustzijn binnen het organisatieonderdeel.

Acties komende jaar
In het komende jaar wordt de e-learning privacy voor het laatste deel van de organisatie uitgerold. Het blijkt nodig iemand aan te wijzen die tijd heeft om zich met uitrol van e-learnings bezig te houden, niet alleen voor privacy maar ook voor informatieveiligheid. Anderhalf jaar na de start van de uitrol e-learning privacy is nog steeds niet de hele organisatie aangesloten terwijl er ook vernieuwde vragen bij zouden moeten komen die weer uitgerold moeten worden, kortom een redelijk continue proces.
Ook ten aanzien van informatieveiligheid zal er meer aandacht moeten zijn voor de basisvaardigheden van medewerkers. Een bewustwordingscampagne n.a.v. de phishing mailaanval is hier onderdeel van.

8 Register van gegevensverwerkingen

Context
Het register van gegevensverwerkingen is een vastlegging van alle soorten verwerkingen van persoonsgegevens door de Regio. In het register is onder meer vastgelegd welke soorten persoonsgegevens er in de verschillende werkprocessen binnen de organisatie worden vastgelegd en verwerkt, wat de rechtmatige grondslag hiervoor is, aan wie deze gegevens worden verstrekt en hoe lang deze gegevens worden bewaard. Dit register is verplicht en geldt als één van de belangrijkste verantwoordingsinstrumenten voor een goede omgang met persoonsgegevens. Het register is continue in beweging omdat er taken bij komen en processen veranderen en in de praktijk vaak anders blijken te lopen dan ooit is opgeschreven.

Voortgang in verslagjaar
Het register is op dit moment in transitie omdat de dienstverlening van de softwareleverancier is gestopt en we overgaan op ontsluiting van het nieuwe DMS-systeem Decos Join.

Acties komende jaar
Vanwege het stoppen van Verifield is het nodig voor het register over te stappen naar een andere oplossing. De belangrijkste functionaliteiten van de software zijn overgenomen in de Regio-inrichting van Decos Join. Het komende jaar is het van belang dat het register van gegevensverwerkingen volledig wordt overgezet naar Decos Join. Het borgen van het register in een applicatie is van belang zodat de FG er met de aandachtsfunctionarissen samen aan kan werken.

9 Processen privacyproof

Context
Het is van belang dat de verwerkingen van de Regio zoals deze in het register van gegevensverwerkingen staan volgens de privacyregels plaatsvinden.
Dit houdt in dat de werkprocessen die persoonsgegevens bevatten, getoetst en ingericht moeten worden volgens de beginselen behoorlijkheid, transparantie, doelbinding, dataminimalisatie (niet meer dan nodig), opslagbeperking (niet langer dan nodig), juistheid, integriteit en vertrouwelijkheid.
Voor een aantal verwerkingen met een hoog risico voor inwoners/medewerkers is de Regio verplicht een uitgebreidere gegevensbeschermingseffectbeoordeling (vooral bekend onder de Engelse afkorting DPIA) uit te voeren. Door het uitvoeren van een DPIA wordt de privacyimpact van de betreffende verwerking zo minimaal mogelijk gehouden. De afhandeling van de (niet-GGD gerelateerde) DPIA's wordt getrokken door de Adviseur Informatie.

Voortgang in verslagjaar
De Adviseur Informatie heeft in 2022 5 uur in de week extra gekregen om DPIA's uit te voeren. Gebleken is dat dit aantal uren te weinig is om de DPIA-kalender uit te kunnen voeren. Bovendien is het in die tijd niet haalbaar om bij het maken van een DPIA alle disciplines te betrekken, hetgeen voor een goede DPIA wel van belang is.
In het afgelopen jaar is er een DPIA gedaan op de processen adviezen en meldingen van Veilig Thuis ten behoeve van de overgang naar een nieuw systeem (Myneva). Ook wordt op het moment van schrijven van dit verslag aan de DPIA voor het DLP de laatste hand gelegd. Op de geïnventariseerde risico's en maatregelen heeft de FG geadviseerd.
Daarnaast zijn in GGD-verband door FG en epidemioloog twee landelijke DPIA's van de Gezondheidsmonitor (Corona Gezondheidsmonitor Jeugd 2021 en Corona Gezondheidsmonitor Jongvolwassenen 2022) op maat gemaakt voor de Regio.[2] Ten slotte zijn in het afgelopen verslagjaar, net als in de voorgaande twee jaren, meerdere DPIA's op landelijk GGD-niveau uitgevoerd i.h.k.v. de bouw van systemen voor de bestrijding van corona. Ook de FG heeft hieraan bijgedragen en de Directeur Publieke Gezondheid hierover geadviseerd.
Ten aanzien van nieuwe Regiotaken die gemeenten bij de Regio beleggen (voor zover daarbij persoonsgegevens worden verwerkt), vindt sinds dit verslagjaar afstemming plaats met de FG's van de regiogemeenten over o.a. AVG-verantwoordelijkheden, risico's en maatregelen. Deze afstemming dient om tot een gezamenlijk FG-advies te komen. In dit verslagjaar is een gezamenlijk advies opgesteld t.a.v. de zorgcoördinator mensenhandel en is een voorbereiding gedaan voor een advies over het Regionaal Expert Team Jeugd (RET).

Acties komende jaar
Er wordt ingezet op spoedige afronding van de DPIA voor het Digitaal Leefplein. Verder moeten dit kalenderjaar nog DPIA's worden uitgevoerd voor de verwerkingen die onder de Wpg vallen. Daarnaast vereisen ook enkele nieuwe niet-wettelijke taken (zoals het RET) DPIA's, die zo nodig in samenwerking met de regiogemeenten zullen worden uitgevoerd. Het zal hierbij nodig kunnen zijn om hiervoor externe partijen in te huren. In januari zal weer bekeken worden welke hoogrisicoverwerkingen dan in aanmerking komen voor een DPIA en worden deze op de DPIA-kalender opgenomen.
Het is wel nodig om de DPIA's meer multidisciplinair uit te voeren dan nu het geval is. Dit kost uiteraard wel meer tijd waar het de Adviseur Informatie dus aan ontbroken heeft.
Voor de beschikbaarheid van iemand die de uitvoering van DPIA's trekt, moeten de uren voor 2023 en verder overigens nog worden geregeld.

Een belangrijk aandachtspunt voor de korte termijn is het goed meenemen van privacy en informatieveiligheid bij de uitrol van Office 365. Het totaal anders werken zorgt voor nieuwe mogelijkheden maar ook risico's op het gebied van privacy en informatiebeveiliging. Zo geeft een grote mailbox in de cloud gebruiksgemak maar daarmee kan tegelijkertijd de trigger wegvallen om informatie (met persoonsgegevens) uit de actieve mailbox te halen wanneer deze niet meer nodig is. Hiervoor moeten spelregels worden gemaakt.

10 Eenduidige registratie voor verantwoordingsplicht

Context
De in de AVG voorgeschreven verantwoordingsplicht houdt in dat je kunt aantonen dat je als organisatie aan de AVG voldoet. Hiervoor is een eenduidige registratie van privacyrelevante gebeurtenissen van belang. Zo is er naast het register van gegevensverwerkingen en het datalekken- en incidentenregister, een registratie van de afgesloten verwerkersovereenkomsten, de ontvangen

[2] Normaal gesproken is er eens per twee jaar een Gezondheidsmonitor waarvoor ook altijd een DPIA wordt gedaan, maar door corona is er momenteel sprake van een jaarlijkse monitor.

verzoeken i.h.k.v. rechten van betrokkenen (zoals inzageverzoeken) en de door de FG gegeven adviezen en reacties daarop door betreffende RVE-manager.

Voortgang in verslagjaar
Afgelopen verslagjaar is verder gewerkt met de eenduidige registratie van privacyrelevante gebeurtenissen door de Regio.

Acties komende jaar
Doordat de verzoeken i.h.k.v. rechten van betrokkenen meer decentraal (per organisatieonderdeel) zijn opgepakt dan tot nu toe het geval was, is de registratie hiervan niet meer zo eenduidig. Daar valt nog een verbeterslag te slaan.

11 Relaties met derde partijen

Context
De Regio werkt met veel verschillende partijen samen. Deze samenwerking kan veel verschillende vormen aannemen. Voor zover in de samenwerking ook persoonsgegevens worden verwerkt, is het voor de AVG van belang hoe de feitelijke verhoudingen tussen partijen zijn. Het goed duiden van de rollen (zelfstandig verwerkingsverantwoordelijke[3], gezamenlijk verwerkingsverantwoordelijken[4] en verwerker) is één van de lastigste uitdagingen van de AVG.
Bij de verwerking van persoonsgegevens maakt de Regio in sommige gevallen gebruik van (digitale) diensten van externe partijen. Er wordt bij verschillende (digitale) werkprocessen gebruik gemaakt van andere organisaties die een opdracht krijgen tot verwerking van persoonsgegevens. Bij verwerking van persoonsgegevens door een derde partij die handelt ten behoeve van de Regio (als verwerkingsverantwoordelijke) en waarbij gegevensverwerking de primaire opdracht is, is de derde aan te merken als verwerker en moeten afspraken worden gemaakt in een verwerkersovereenkomst.[5]
Overigens is niet voor elke uitbesteding van werk een verwerkersovereenkomst nodig. Als de derde partij zelf bepaalt waarvoor ze persoonsgegevens verwerkt en welke gegevens dat zijn dan is die partij waarschijnlijk zelf verwerkingsverantwoordelijke en is een verwerkersovereenkomst dus niet op zijn plaats.
In relatie tot de regiogemeenten is het van belang of taken gedelegeerd dan wel gemandateerd zijn aan de Regio. Het DB is de verwerkingsverantwoordelijke in de zin van de AVG voor de door de regiogemeenten via delegatie overgedragen taken. Dit betekent dat zij eindverantwoordelijk is voor alles wat te maken heeft met de bescherming van persoonsgegevens binnen de Regio. Voor de taken die in mandaat aan de Regio zijn gegeven blijft de gemeente de verwerkingsverantwoordelijke en is de Regio ofwel verwerker ofwel gezamenlijk verwerkingsverantwoordelijke (samen met de regiogemeente die de verwerkingsverantwoordelijkheid bij mandatering nooit kwijt raakt).
Het zorgen dat verwerkersovereenkomsten op een juiste wijze worden afgesloten (met het beschikbare Word-sjabloon) is een verantwoordelijkheid van de RVE's/organisatieonderdelen zelf. FG en juridisch adviseurs zijn beschikbaar voor beoordelen van de inhoud.
Er zijn in het kader van de AVG nog andere verhoudingen met derde partijen mogelijk waarvoor mogelijk zaken met elkaar overeengekomen moet worden.

[3] Een verwerkingsverantwoordelijke stelt het doel van de verwerking vast en de middelen ervoor, dat wil zeggen het hoe en waarom van de verwerking.
[4] Van gezamenlijke verwerkingsverantwoordelijkheid is sprake bij een gezamenlijke deelname van twee of meer entiteiten aan de vaststelling van het doel en de middelen van een verwerkingsactiviteit.
[5] In deze overeenkomst worden afspraken gemaakt over de verwerking van persoonsgegevens. In de verwerkersovereenkomst worden onderwerp, duur, aard en doel van de verwerking vastgelegd met daarbij het soort persoonsgegevens en de getroffen technische en organisatorische maatregelen om de verwerkingen veilig te stellen en de persoonsgegevens en privacy van betrokkenen te beschermen.

Voortgang in verslagjaar
Nog te vaak blijkt dat verwerkersovereenkomsten uiteindelijk niet zijn afgesloten. Ook komt het voor dat de standaardteksten van de bijlagen niet zijn aangepast aan de uitbestede verwerking. Daarnaast is gebleken dat bij het beleggen van taken bij de Regio de bevoegdheid om persoonsgegevens te verwerken niet altijd duidelijk is vastgelegd.

Acties komende jaar
RVE's/organisatieonderdelen zullen meer in de lead moeten zijn bij het (goed) afsluiten van verwerkersovereenkomsten met partijen die als een verwerker van ons zijn aan te merken. Organisatieonderdelen worden gevraagd nieuwe gegevensuitwisselingen met derde partijen altijd voor te leggen aan de betreffende juridisch adviseur.
Er komt een nieuw sjabloon van de verwerkersovereenkomst zodat medewerkers beter weten wat ze moeten invullen en deze beter aansluit op de verschillende soorten uitbestedingen (zoals ICT en dienstverlening). Voor het aanpassen van de verwerkersovereenkomst is aangesloten bij het nieuwe inkoopbeleid en bijbehorende aanpassing van sjablonen.
Ten slotte is het van belang de gemeenschappelijke regeling te verduidelijken ten aanzien van de gebruikte juridische constructie (zoals delegatie, mandatering, dienstverlening, aanwijzing) en de consequenties daarvan voor de AVG-rolverdeling.

12 Privacybeleid

Context
Wanneer een organisatie op grote schaal bijzondere persoonsgegevens verwerkt dient die organisatie een privacybeleid op te stellen en te hanteren. Binnen de Regio verwerken een aantal onderdelen op grote schaal bijzondere persoonsgegevens, voornamelijk gezondheidsgegevens. Daarom is het hebben van een privacybeleid voor de Regio een verplichting en dit beleid is er sinds 2021. Het privacybeleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en zowel geautomatiseerde als handmatige verwerkingen van persoonsgegevens door de Regio.
Het privacybeleid is een belangrijk instrument om in vast te leggen hoe we bij de Regio met persoonsgegevens om gaan. Het is een intern document en is een handleiding voor medewerkers over werken met persoonsgegevens.

Voortgang in verslagjaar
Voor het privacybeleid is in het afgelopen verslagjaar een start gemaakt met het updaten van het beleid, wat een levend document is.

Acties komende jaar
Komend jaar is het belangrijk het privacybeleid bij de verschillende organisatieonderdelen goed bekend te maken. Hiervoor zal het beleid meer geconcretiseerd worden per organisatieonderdeel om het herkenbaar te maken voor de uitvoering. Dit kan door het maken van een versimpelde weergave van het beleid met RVE/organisatieonderdeel-specifieke aandachtspunten en door dit vervolgens met interactieve sessies bij de RVE's/organisatieonderdelen te laten landen. De FG gaat hier samen met juridisch adviseurs en de RVE's/organisatieonderdelen mee aan de gang.
Het privacybeleid dient regelmatig geëvalueerd te worden en zo nodig aangepast. Voor komend jaar staat dat op de planning.

13 Informatieplicht verwerkingen algemeen en websites

Context
Het is van belang dat de verwerkingsverantwoordelijke de personen waarvan zij persoonsgegevens

verwerkt (voornamelijk inwoners en medewerkers) informeert over de verwerking en de rechten die zij hierbij kunnen uitoefenen. Een privacyverklaring op de website is hiervoor het meest logische middel.

Voortgang in verslagjaar
Ter invulling van het recht van inwoners om transparante informatie over de verwerking van persoonsgegevens te ontvangen, is er een algemene privacyverklaring voor alle verwerkingen van de Regio. Om te voldoen aan de informatieplicht uit de AVG is echter specifiekere informatie (toegespitst op de verwerking/set van verwerkingen) nodig. Daarom is afgelopen jaar een sjabloon gemaakt voor drie soorten privacyverklaringen, voor een website van een organisatieonderdeel, een thema en van een campagne. Afgelopen verslagjaar is hier met een aantal RVE's/organisatieonderdelen al een slag mee geslagen.

Acties komende jaar
Komend jaar moet er voor alle organisatieonderdelen die een website hebben een specifieke privacyverklaring komen omdat inwoners de verschillende organisatieonderdelen als losse organisaties ervaren en aparte verklaringen per organisatie beter toegankelijk zijn en dan pas voldoen aan de AVG. Daarnaast zal er een privacyverklaring voor medewerkers gemaakt moeten worden die de verwerkingen van persoonsgegevens op het werk beschrijft.

14 Verzoeken i.h.k.v. rechten van betrokkenen

Context
Iedereen van wie persoonsgegevens worden verwerkt, heeft een aantal rechten t.a.v. die verwerking, de zogenaamde 'rechten van betrokkenen'. Deze rechten staan in de AVG, maar enkele komen ook (soms net iets anders) voor in de materiewetgeving die op bepaalde organisatieonderdelen van toepassing is.[6] De bekendste rechten betreffen het recht om een verzoek tot inzage, een verzoek tot rectificatie of een verzoek tot verwijdering of vernietiging in te dienen.

Voortgang in verslagjaar
Er werd in het afgelopen verslagjaar één verzoek i.h.k.v. rechten van betrokkenen onder de AVG ontvangen dat uiteindelijk onder de Wet op de geneeskundige behandelovereenkomst (Wgbo) bij Jeugd en Gezin is afgehandeld.
Daarnaast werden zoals altijd meerdere inzage- en vernietigingsverzoeken door Veilig Thuis ontvangen. Ook inzageverzoeken in het rittenformulier bij RAV komt regelmatig voor. Deze verzoeken bij Veilig Thuis en RAV zijn niet onder de AVG afgehandeld maar onder de eigen materiewet, respectievelijk Wmo 2015 en Wgbo. Ten slotte is bij het Zorg- en Veiligheidshuis één verzoek om inzage ingediend waarbij doorverwezen is naar de betreffende ketenpartner en verzoeker is uitgenodigd om zelf aan tafel te komen zitten.
Door aanpassing van de privacyverklaringen bij enkele organisatieonderdelen worden verzoekers geholpen bij het benoemen van het juridisch kader (AVG of materiewet) waar zij het meest aan hebben.

15 Datalekken

Context
Een 'informatieveiligheidsincident' is een datalek indien sprake is van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is.

[6] Grofweg komt het erop neer dat betrokkenen bij een beroep op de AVG hun rechten kunnen laten gelden t.a.v. losse persoonsgegevens, terwijl bij een beroep op de Wet op de geneeskundige behandelovereenkomst (Wgbo), Jeugdwet of Wmo 2015 de rechten gelden t.a.v. het document/dossier zelf.

De organisatie stimuleert het intern melden van mogelijke datalekken bij het Team Privacyincidenten. Van de afhandeling van meldingen wordt de organisatie alleen maar beter.
Indien er een risico is voor inwoners of medewerkers moet het datalek worden gemeld aan de AP. Indien dat risico hoog is, moet het datalek ook worden gemeld aan degene op wie de persoonsgegevens betrekking hebben.

Voortgang in verslagjaar
Er is zoals elk jaar een evaluatie uitgevoerd van het proces voor het afhandelen van meldingen van (mogelijke) datalekken. Deze evaluatie heeft geleid tot een aanpassing van de samenstelling van het Team Privacyincidenten. Tevens zijn alle meldingen inhoudelijk geëvalueerd. Hierbij is de conclusie getrokken dat strikter gebruik van Zivver of een andere veilige mailoplossing een hoop datalekken zou kunnen voorkomen dan wel beperken. Verder is gebleken dat het afhandelen van datalekken de FG te veel tijd kost en dat gaat ten koste van het echte FG-werk.
In het afgelopen verslagjaar zijn intern negenendertig informatieveiligheidsincidenten gemeld. Dit zijn negen incidenten minder dan in het verslagjaar hiervoor. Van de meldingen bleek het in twintig gevallen daadwerkelijk om een datalek te gaan. De meeste datalekken deden zich voor bij Veilig Thuis. Van deze twintig datalekken was in twaalf gevallen sprake van een risico voor betrokkenen waardoor gemeld moest worden aan de Autoriteit Persoonsgegevens. Van deze twaalf gevallen is zevenmaal melding aan betrokkenen gemaakt, het merendeel uit zorgvuldigheid, slechts twee keer omdat er werkelijk een hoog risico was.
De meest voorkomende datalekken vielen in de categorieën ‘versturen van persoonsgegevens aan verkeerde ontvanger’, op ruime afstand gevolgd door ‘toegankelijkheid van persoonsgegevens voor niet-bevoegde persoon’. Het ging in het eerste geval om het versturen van brieven of mails naar de verkeerde ontvanger. In het tweede geval ging het vaak om applicaties waartoe te ruime toegang was ingesteld. Twee datalekken sprongen eruit omdat ze niet vaak voorkomen. Het gaat om de phishing mailaanval waarbij mailboxen van twee collega’s zijn gehackt en om de fraude met corona QR-codes waarbij dossiers van patiënten onrechtmatig zijn gewijzigd.

Acties komende jaar
Zivver (of een andere veilig mailen-oplossing) moet meer op de kaart worden gezet en verplicht gesteld worden voor het verzenden van persoonsgegevens naar buiten de Regio.
Er zal aan het CMT worden voorgesteld om aandachtsfunctionarissen privacy ook een rol te geven in de inventarisatiefase bij een privacyincident binnen de eigen RVE/organisatieonderdeel. De beoordeling vindt dan nog steeds plaats binnen het Team Privacyincidenten.

16 Informatieveiligheid

Context
Een goede inrichting van informatieveiligheid is belangrijk voor een optimale bescherming van persoonsgegevens.

Voortgang in verslagjaar
Door een phishing mailaanval in april 2022 is de Regio noodgedwongen overgegaan op vervroegde introductie van multi factor authenticatie (MFA) om ervoor te zorgen dat je meer nodig hebt dan alleen een wachtwoord om in de systemen te komen.

Acties komende jaar
De landelijk aangezwengelde professionaliseringsslag van de GGD’en heeft tot nieuwe impulsen voor informatieveiligheid geleid. Zo bestaat de intentie om met de GGD voor NEN 7510 gecertificeerd te worden. Hiervoor is echter wel eerst nodig de basis (het applicatielandschap) op orde te hebben en

daar is de Regio op het moment van schrijven met de implementatie van Office 365 nu nog heel druk mee bezig.

17 Oordeel over afgelopen jaar en aandachtspunten komende periode

Het afgelopen verslagjaar is de afstemming met alle onderdelen van de Regio op het gebied van privacy weer een stuk beter geworden, mede doordat corona iets minder tijd vroeg. Dit geldt vooral voor de afstemming met privacygevoelige onderdelen als Sturing/Sociaal Domein, Zorg- en veiligheidshuis, WSP en RBL.
Over de Office 365 implementatie zijn zorgen op het gebied van inregelen van informatieveiligheid- en privacymaatregelen. Maar daarmee wordt nu als het goed is een inhaalslag gepleegd. De uitrol van de e-learning privacy verloopt te langzaam doordat het behoorlijk arbeidsintensief is gebruikers op te voeren en er niemand is die hier voldoende tijd voor heeft, dat moet anders. DPIA's zullen meer multidisciplinair en in voorkomende gevallen samen met Regiogemeenten moeten worden opgepakt.
Ten slotte leeft het in 2021 vastgestelde privacybeleid nog niet genoeg.

Komend jaar is het verder operationaliseren van het privacybeleid binnen de organisatieonderdelen van belang. De aandachtsfunctionarissen privacy spelen hierin een belangrijke rol.
Met het afnemen van de e-learning en een campagne n.a.v. de phishing mailaanval moet meer aan bewustzijn worden gedaan, op het gebied van privacy maar ook op het gebied van informatieveiligheid in het algemeen.
Zivver moet beter worden gebruikt en daarover moet voorlichting komen. Het consequent gebruik van Zivver zorgt voor het veilig verzenden van persoonsgegevens naar buiten de Regio en kan het aantal en impact van datalekken beperken.

18 Aanbeveling

De FG doet wederom een aanbeveling voor het structureel organiseren van meer capaciteit voor het Regiobreed proactief oppakken van privacygerelateerde zaken. Deze aanbeveling moet zorgen voor een betere borging van de privacy van burgers en medewerkers. Op dit moment is de FG bestendig met proactieve privacyzaken bezig en heeft de Adviseur Informatie hiervoor 5 uren beschikbaar.

Meer armslag voor privacytaken is om meerdere redenen van belang.
Allereerst mag de FG zich vanuit zijn toezichthoudende taak maar beperkt met uitvoerende privacytaken bezig houden.
Daarnaast heeft het DB als verwerkingsverantwoordelijke de taak om de FG te ondersteunen om zijn werk goed te kunnen uitvoeren onder andere door hem middelen te verschaffen (zoals genoemd in artikel 38 lid 2 AVG). Op het moment dat de noodzakelijke uitvoerende werkzaamheden door de FG zelf uitgevoerd moeten worden, komt de uitvoering van zijn wettelijke taken in het gedrang.
Verder is het zo dat de FG extra toezichthoudende taken erbij heeft gekregen onder de Wpg die vanaf 2023 ook echt uitgeoefend zullen moeten worden. En de nauwere samenwerking met de FG's bij de regiogemeenten ten aanzien van advisering over nieuwe taken die bij de Regio worden ontwikkeld zorgt ook voor een extra beroep op de FG van de Regio.
Ten slotte zijn er externe oorzaken die maken dat er binnen de gemeentelijke overheid en ook de Regio een professionaliseringsslag moet worden gemaakt. Niet alleen op het gebied van informatieveiligheid, maar ook op privacygebied.

Dit betekent o.a. dat uitvoerende privacytaken (zoals het uitvoeren van DPIA's en de uitrol en doorontwikkeling van e-learning), op een kortere termijn dan tot nu haalbaar is gebleken, goed ingevuld

moeten worden. De uren die hiervoor in 2022 beschikbaar waren, waren niet voldoende en deze zijn vanaf 2023 nog niet geregeld. Minimaal 8 uren en het liefst 16 uren zijn benodigd om dit beter op de kaart te zetten.
Het beschikbaar hebben van iemand voor uitvoerende privacytaken kan de organisatie bovendien helpen om de onafhankelijke adviezen van de FG in een werkbare oplossing te gieten.

Als er voor wordt gekozen om de gevraagde capaciteit niet beschikbaar te maken is de consequentie dat de Regio niet duurzaam volledig kan voldoen aan de AVG. De bescherming van persoonsgegevens van inwoners en medewerkers kan dan niet optimaal worden verwezenlijkt. Daarmee kan de Regio kwetsbaar zijn voor handhavende maatregelen van de externe toezichthouder en aansprakelijkstellingen door inwoners.

Bijlage 1 Formele FG-adviezen

Onderwerp	Advies FG	Verwerkings-verantwoordelijke	Reactie verwerkingsverantwoordelijke
Gebruik slecht geïsoleerde vergaderzalen voor gevoelige overleggen	Zorg ervoor dat de vergaderzalen met schuifbare wanden goed geïsoleerd zijn voor vertrouwelijke gesprekken.	Algemeen directeur	Overgenomen, vergaderzalen worden nu beter afgesloten met de rubberen strips aan de randen van de wanden.
Proefconversie (met echte persoonsgegevens) JGZ naar Amsterdam	Zorg ervoor dat enkel de allerlaatste proefconversie (vlak voor de echte) met echte persoonsgegevens plaats vindt.	J&G	Gemotiveerd niet overgenomen
Proefconversie (met echte persoonsgegevens) van RegiPro naar Myneva	Zorg ervoor dat enkel de allerlaatste proefconversie (vlak voor de echte) met echte persoonsgegevens plaats vindt.	Veilig Thuis	Gemotiveerd niet overgenomen
Advies aanzetten MFA BySpy	Zet multi factor authenticatie (MFA) aan op de webapplicatie BySpy waarin politiegegevens door de boa's van de GAD worden verwerkt.	GAD	Overgenomen
Diverse beslissingen t.a.v. bestrijding van corona	Adviezen over organisatie- en systeemkeuzes bij bestrijding van corona	GGD	Wisselend