Regio Gooi en Vechtstreek

MEMO

Verslag Functionaris Gegevensbescherming over periode juli 2020 - juni 2021

Algemeen	
Aan	CMT, DB, AB
Van	Anne Cnossen
Datum	21 juli 2020
Verspreiden	Nee
Kenmerk	21.0005069

Samenvatting

Dit is het derde verslag van de Functionaris Gegevensbescherming aan het Dagelijks Bestuur. Het verslag beslaat de periode juli 2020 tot en met juni 2021.
Het volledige verslagjaar stond op het gebied van privacy grotendeels in het teken van corona. Vooral de ondersteuning van de GGD op privacygebied in de afstemming met andere GGD'en en de brancheorganisatie GGD GHOR Nederland vroeg om een enorme tijdsinvestering van de Functionaris Gegevensbescherming. Ook de afwikkeling van de landelijke datadiefstal bij de GGD die in januari 2021 aan het licht kwam en de vervolgacties met betrekking tot inrichten van veiligere systemen heeft veel tijd in beslag genomen.
Op het gebied van implementatie van de Algemene Verordening Gegevensbescherming (AVG) is ondanks corona toch nog enige voortgang geboekt.
Het privacybewustwordingsproces van de Regio is weer een stap verder gekomen. Zo is in de eerste helft van 2021 een start gemaakt met de uitrol van de e-learning privacy met als doel het vergroten van de digitale weerbaarheid van de Regio en haar medewerkers. Daarnaast is bewustwording vergroot door advisering door juridisch adviseurs en de Functionaris Gegevensbescherming en door de nasleep van datalekmeldingen. Er zijn dit verslagjaar veel meer interne meldingen van mogelijke datalekken gedaan dan in eerdere jaren. Er is een evaluatie uitgevoerd op de gemelde datalekken en op de procedure tot afhandeling van deze meldingen. Er is via het intranet meer aandacht besteed aan het 'waarom' van privacy in plaats van alleen focus op de uit te voeren regels.
In samenspraak met de FG van GGD Flevoland zijn een aantal privacyaspecten van de RAV verbeterd. Mede door deze maatregelen is de NEN-certificering van de RAV weer verlengd.
Ook zijn weer enkele risicoanalyses uitgevoerd op verwerkingen van persoonsgegevens met een hoog risico. Er zijn door RVE/teammanagers enkele nieuwe aandachtsfunctionarissen privacy benoemd. In de eerste helft van 2021 is door de Functionaris Gegevensbescherming (in samenspraak met de RVE's) een nieuw privacybeleid opgesteld, welk beleid eind juni 2021 door het Dagelijks Bestuur is vastgesteld.
Bij de oprichting van Vervoer Gooi en Vechtstreek B.V. is geadviseerd over een privacyproof start van de werkzaamheden. Op de werkzaamheden vanaf 1 januari 2021 wordt in een apart FG-verslag van Vervoer Gooi en Vechtstreek B.V. ingegaan.
Ten slotte werd in de eerste helft van 2021 bekend dat de Regio een audit voor de Wet politiegegevens dient uit te voeren vanwege het feit dat zij BOA's in dienst heeft. Hiervoor zijn de benodigde stappen inmiddels in de lijn belegd.

Komend jaar is het oppakken van zaken waarvoor in afgelopen jaar te weinig tijd beschikbaar was van belang. Het gaat om het verder oppakken van de uitvoering van privacywetgeving en het nieuwe

privacybeleid door de RVE's. De aandachtsfunctionarissen privacy spelen hierin een belangrijke rol. Er wordt opnieuw geïnvesteerd in scholing van aandachtsfunctionarissen. Tegelijkertijd moet ook het register van gegevensverwerkingen op één plek (een applicatie) beschikbaar komen zodat aandachtsfunctionarissen en Functionaris Gegevensbescherming hier samen aan kunnen werken. Het bewustwordingstraject moet een verdere boost krijgen door de volledige uitrol van de e-learning. Er zullen nieuwe risicoanalyses op de verwerkingen met een hoog risico voor inwoners en medewerkers worden uitgevoerd. Verder zal de Functionaris Gegevensbescherming toezien op de verantwoordelijkheid van RVE's voor maken van afspraken met derde partijen en het goed invulling geven aan de informatieplicht t.a.v. de verwerkingen van persoonsgegevens.
Het verslag bevat ten slotte een aanbeveling over 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 derde verslag van de Functionaris Gegevensbescherming (hierna: FG) aan het Dagelijks Bestuur (hierna: DB). In de Algemene Verordening Gegevensbescherming (hierna: AVG) 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 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 2020 tot en met juni 2021) 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 privacybeleid. 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.

Het afgelopen verslagjaar heeft het coronavirus ons in haar greep gekregen en gehouden. Bij de bestrijding van corona wordt ook aan veel privacygerelateerde onderwerpen geraakt, met name omdat de GGD hiervoor allerlei nieuwe processen heeft moeten optuigen.
Een ander punt dat in afgelopen jaar veel landelijke aandacht trok was de toeslagenaffaire. N.a.v. de toeslagenaffaire zal de (rijks)overheid goed moeten kijken naar processen en systemen die een discriminerende invalshoek kunnen hebben. Ook binnen de Regio is het van belang om goed te kijken naar het gebruik van algoritmes en zwarte lijsten. Bij de Regio is voor zover bekend daar nu geen sprake van, maar het is ook van belang dat dat zo blijft.
Een laatste gebeurtenis die veel impact heeft gehad betreft de datadiefstal bij GGD GHOR Nederland. Deze zaak benadrukt nog eens het belang van een goede inrichting van privacy en security. Vanaf nu zal voor iedereen duidelijk zijn dat je alleen toegang tot/rechten in applicaties met gevoelige gegevens kunt krijgen indien dat noodzakelijk is om het werk te kunnen uitvoeren.
Bovengenoemde ontwikkelingen hebben gezorgd voor het inzetten een overheidsbrede professionaliseringsslag. Daardoor is het van belang informatieveiligheid en privacy ook bij de Regio hoog op de agenda te zetten en houden.

2 Organisatorische inbedding

Alle RVE-managers hebben één of meerdere aandachtsfunctionarissen privacy benoemd om hen te ondersteunen in hun privacytaken. Inmiddels zijn door RVE-/teammanagers Inkoop en Contractbeheer, Maatschappelijke Dienstverlening en Regionaal Bureau Leerlingzaken enkele nieuwe aandachtsfunctionarissen privacy benoemd. De aandachtsfunctionaris is het eerste aanspreekpunt voor privacy voor zijn/haar eigen RVE en voor de FG. Zij signaleren wijzigingen in de verwerkingen van persoonsgegevens en coördineren voor hun RVE de afhandeling van de organisatiebrede verzoeken (zoals verzoeken om inzage) die inwoners en medewerkers vanuit de AVG bij de Regio kunnen indienen. Een aantal keren per jaar spreekt de FG afzonderlijk met de verschillende aandachtsfunctionarissen privacy.

Acties komende jaar
Komend jaar krijgen de aandachtsfunctionarissen privacy opnieuw een opleiding privacy. Hierin is ook het nieuwe privacybeleid verwerkt. Door het goed positioneren van de aandachtsfunctionarissen wordt de verdere uitvoering van privacywetgeving door de RVE's naar verwachting gemakkelijker. Pas als het

bij de RVE's geolied gaat lopen, is een belangrijke voorwaarde voor een duurzame privacyinrichting vervuld.

3 Kennis en kunde privacy

Afgelopen jaar hebben de diverse functionarissen die zich met privacy bezig houden hun kennis van privacy onderhouden.
Uit het netwerk met de FG's en Privacy Officers van de regiogemeenten komen nuttige ervaringen en best practices naar voren die ook door de Regio worden benut.
De juridisch adviseurs en FG hebben weer diverse opleidingen en cursussen op het gebied van privacy gevolgd. Ook elders in de organisatie zit kennis over privacy, zoals bij de Adviseur Informatie die ook gecertificeerd CIPP/E en CIPT (certificering voor de informatieveiligheidskant van privacy) is.
Kortom, bij de Regio is een voldoende kennisbasis om privacy en privacyvraagstukken afdoende aan te pakken.

Acties komende jaar
Komend jaar wordt weer geïnvesteerd in het privacykennisniveau van de aandachtsfunctionarissen privacy. Hierdoor wordt geborgd dat uitvoering van de privacyregelgeving in de organisatie verder wordt verbeterd.

4 Advisering, informatieverstrekking en voorlichting

In het afgelopen verslagjaar heeft de FG diverse informele en formele adviezen gegeven aan de organisatie. Daarnaast heeft de FG ook advies gegeven ten aanzien van geïnventariseerde risico's die naar voren kwamen bij het uitvoeren van privacyrisicoanalyses, ook wel DPIA's. Hierop wordt in een apart hoofdstuk (Processen AVG-proof) ingegaan.
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.
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. In het kader van de bestrijding van corona is er intensief contact tussen FG en Directeur Publieke Gezondheid, waarbij veel 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.
Ook werd vaak advies verstrekt bij vragen over het AVG-proof inrichten van verschillende werkprocessen, het ontwikkelen van beleid, procedures en werkinstructies.

5 Toezicht op toepassing en naleving AVG

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 de datadiefstal bij GGD GHOR Nederland. Verder is in 2021 duidelijk geworden dat de regio in 2021 gestart moet zijn met een interne en vervolgens externe audit voor de Wet politiegegevens. De FG heeft hierin geen toezichthoudende taak. Ter voorbereiding op de audit zijn de afgelopen periode de nodige maatregelen getroffen.

Acties komende jaar
Het intensiveren van de één op één gesprekken tussen FG en aandachtsfunctionarissen privacy/RVE-managers is komend jaar weer van belang. Deze gesprekken zijn ook te beschouwen als een vorm van toezicht. Daarnaast zal voor de audit Wet politiegegevens een traject doorlopen moeten worden van inrichten van procedures, werken volgens procedures, interne audit, verbeterplan en vervolgens de externe audit.

6 Bewustwording

Er is het afgelopen verslagjaar op verschillende manieren aan privacybewustwording gedaan. In de Leerhuislunches en op het intranet is regelmatig stilgestaan bij privacy (zoals de richtlijnen om veilig thuis te kunnen werken). Door de juridisch adviseurs zijn en worden op maat gemaakte trainingen gegeven aan verschillende RVE's.
Begin 2021 is door het CMT vastgesteld dat digitale weerbaarheid (op het gebied van privacy en informatiebeveiliging algemeen) een vereiste competentie is van alle medewerkers. In de eerste helft van 2021 is een start gemaakt met de uitrol van de e-learning privacy met als doel het vergroten van de digitale weerbaarheid van de Regio en haar medewerkers. Het was aanvankelijk de bedoeling alle RVE's voor de zomervakantie 2021 met de e-learning te laten starten, maar dit is een behoorlijk tijdrovende klus waardoor dit niet is gelukt.
Ook worden vragen over privacy en afwikkeling van datalekken aangegrepen om privacybewustwording bij management en medewerkers te vergroten. De FG spreekt normaal gesproken meerdere keren per jaar apart met de aandachtsfunctionarissen privacy van elke RVE. Daarnaast wordt eens per jaar een gesprek met de RVE-managers gepland. Beide momenten worden gebruikt om daar o.a. aandacht te vragen voor het belang van blijvend privacybewustzijn binnen de RVE.
Deze gesprekken zijn afgelopen jaar door tijdgebrek en het op afstand werken niet allemaal consequent gevoerd.

Acties komende jaar
In het komende jaar wordt de e-learning privacy in de hele organisatie uitgerold. Ook zal er meer aandacht moeten zijn voor de basisvaardigheden van medewerkers ten aanzien van informatieveiligheid. Het intensiveren van de één op één gesprekken tussen FG en aandachtsfunctionarissen privacy/RVE-managers is komend jaar weer van belang.

7 Register van gegevensverwerkingen

In het register van verwerkingen 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 op dit moment deels in Excel en deels in de AVG compliance software Kluwer Verifield opgenomen. Het is niet handig dat de verwerkingen over twee lokaties verdeeld zijn. Bedoeling is dat het volledig wordt overgezet naar de software zodat het register naar de aandachtsfunctionarissen privacy kan worden ontsloten. De tijd om dit te doen heeft afgelopen jaar ontbroken.

Acties komende jaar
Het komende jaar is het van belang dat het register van gegevensverwerkingen verder wordt overgezet naar Verifield. Het borgen in een applicatie is van belang om er met de aandachtsfunctionarissen samen aan te kunnen werken. Daarnaast is het opnemen van alle verwerkingen in Verifield nodig om

het proces van rechten van betrokkenen (o.a. inzage- en verwijderverzoeken) dat door Verifield wordt ondersteund, efficiënt te kunnen uitvoeren.

8 Processen AVG-proof

Net als in het voorgaande verslagjaar is afgelopen verslagjaar beoordeeld of de verwerkingen zoals deze in het register van gegevensverwerkingen staan wel privacyvriendelijk genoeg plaatsvinden. Dit houdt in dat de werkprocessen die persoonsgegevens bevatten (zoals te vinden in het register van verwerkingen) 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 heeft de FG vastgesteld dat de Regio verplicht is een uitgebreidere gegevensbeschermingseffectbeoordeling (vooral bekend onder de Engelse afkorting DPIA) uit te voeren. Dit is een verplichting als de verwerking een hoog risico voor inwoners/medewerkers inhoudt. Door het uitvoeren van een DPIA wordt de privacyimpact van de betreffende verwerking zo minimaal mogelijk gehouden. De afhandeling van DPIA's wordt getrokken door de Adviseur Informatie.
In het afgelopen jaar zijn de DPIA Gezondheidsmonitor Volwassenen en Ouderen en Zorg- en Veiligheidshuis geheel afgerond. Op de geïnventariseerde risico's en maatregelen heeft de FG geadviseerd. De DPIA voor het Digitaal Leefplein is gestart, maar kon vanwege afhankelijkheid van de ISAE 3402 certificering nog niet worden afgerond. Verder zijn in het afgelopen verslagjaar meerdere DPIA's op landelijk niveau uitgevoerd i.h.k.v. de bestrijding van corona. Ook de FG van de GGD Gooi en Vechtstreek heeft hieraan bijgedragen en de Directeur Publieke Gezondheid hierover geadviseerd.

Acties komende jaar
Door het opnemen van alle verwerkingen in Verifield zullen op alle verwerkingen van persoonsgegevens kleine risicoanalyses worden uitgevoerd. Er wordt ingezet op afronding van de DPIA voor het Digitaal Leefplein. Ook komend jaar zal bekeken worden welke hoogrisicoverwerkingen verder nog in aanmerking komen voor een DPIA. Zo mogelijk worden de DPIA's opgenomen in de interne audit agenda die nog in de maak is.

9 Eenduidige registratie voor verantwoordingsplicht

Afgelopen verslagjaar is verder gewerkt met de eenduidige registratie van privacyrelevante activiteiten door de Regio. Hiermee wordt tegemoet gekomen aan de door de AVG voorgeschreven verantwoordingsplicht. Zo is er naast het register van gegevensverwerkingen en het datalekkenregister, een registratie van de afgesloten verwerkersovereenkomsten, de ontvangen verzoeken i.h.k.v. rechten van betrokkenen en de door de FG gegeven adviezen en reacties daarop door betreffende RVE-manager. Vooral de registratie ten aanzien van de ontvangen (verwijder)verzoeken als gevolg van de datadiefstal bij GGD GHOR Nederland is een uitdaging geweest.

10 Relaties met derde partijen

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.
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. Verwerking van persoonsgegevens door een derde partij die handelt ten behoeve van de Regio en waarbij gegevensverwerking de primaire opdracht is, moet worden geregeld in een verwerkersovereenkomst.

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. Overigens is niet voor elke uitbesteding van werk een verwerkersovereenkomst nodig.
De Algemene inkoopvoorwaarden van de Regio zijn inmiddels geschikt gemaakt voor zowel de situatie dat een leverancier verwerker is als voor de situatie dat leverancier zelf verwerkingsverantwoordelijke is. Voorheen gingen de voorwaarden ervan uit dat een leverancier die persoonsgegevens verwerkt altijd verwerker is. In aanbestedingstrajecten kamen daar vaak vragen over. Deze nieuwe inkoopvoorwaarden zijn op dit moment nog niet vastgesteld.
Het zorgen dat verwerkersovereenkomsten op een juiste wijze worden afgesloten (met het beschikbare Word-sjabloon) is een verantwoordelijkheid van de RVE's zelf. FG en juridisch adviseurs zijn beschikbaar voor beoordelen van de inhoud. 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.
Er zijn in het kader van de AVG nog andere verhoudingen met derde partijen mogelijk waarvoor iets met elkaar overeengekomen moet worden.
Het goed duiden van de rollen (zelfstandig verwerkingsverantwoordelijke, gezamenlijk verwerkingsverantwoordelijken en verwerker) is één van de lastigste uitdagingen van de AVG.

Acties komende jaar
RVE's 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. De komende tijd verwachten FG en juridisch adviseurs stappen te kunnen zetten bij het maken van een beoordelingskader dat gebruikt kan worden om de rolverdeling met derde partijen (niet zijnde een verwerker) te beoordelen. Waarna dit vervolgens uitgedragen kan worden naar de organisatie. In de tussentijd moeten RVE's hierop ook al scherp blijven en nieuwe gegevensuitwisselingen met derde partijen voorleggen aan de juridisch adviseurs.

11 Privacybeleid

Afgelopen jaar is het privacybeleid van de Regio opgesteld en vastgesteld. 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. Het oude Reglement Bescherming Persoonsgegevens ging nog uit van de indeling van het Gewest en van de voorganger van de huidige privacywetgeving.
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.

Acties komende jaar
Komend jaar wordt ervoor gezorgd dat het privacybeleid binnen de Regio goed bekend is. Ook 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-specifieke aandachtspunten en door dit vervolgens met interactieve sessies bij de RVE's te laten landen. De FG gaat hier samen met juridisch adviseurs en de RVE's mee aan de gang.

12 Informatieplicht verwerkingen algemeen en websites

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. De AVG stelt regels over de informatie die aan inwoners en medewerkers moet worden verstrekt (zoals doel, grondslag, ontvangers en bewaartermijnen van de verwerking) en het moment waarop dat moet gebeuren.
De RVE's zijn verantwoordelijk voor het verstrekken van transparante informatie over verwerkingen van persoonsgegevens die zij doen (ook verwerkingen via een webformulier op een website bijvoorbeeld).

Acties komende jaar
Komend jaar moet de algemene privacyverklaring worden aangevuld met specifieke privacyverklaringen per RVE omdat inwoners de verschillende organisatieonderdelen als losse organisaties ervaren en aparte verklaringen per organisatie beter toegankelijk zijn en dan pas voldoen aan de AVG.
Anders dan nu zullen we toe moeten naar meer specifieke informatie in privacyverklaringen die meer zegt over de verwerkingen binnen een bepaalde RVE (voor de websites van de Regio-onderdelen) of themawebsite. Hierbij kunnen we een raamverklaring als basis gebruiken om de uniformiteit te behouden. De aandachtsfunctionarissen privacy en FG zullen hierin samen optrekken.
Daarnaast zal er een privacyverklaring voor medewerkers gemaakt moeten worden die de verwerkingen van persoonsgegevens op het werk beschrijft.

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

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 RVE's van toepassing is. 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.

Het toepasselijk wettelijk kader, is bepalend voor hoe je een verzoek om inzage, rectificatie of verwijdering moet behandelen en ook in welke vorm de beslissing gegoten wordt. Als het een algemeen verzoek is of als de AVG wordt genoemd dan is de AVG van toepassing. Wordt gevraagd om inzage of verwijdering van een medisch, jeugd- of Veilig Thuis-dossier dan is respectievelijk de Wet op de geneeskundige behandelingsovereenkomst (Wgbo), Jeugdwet of Wmo 2015 het wettelijk kader.
Bij een verzoek om inzage betekent dit, dat een afschrift van de persoonsgegevens (bij AVG als wettelijk kader) of het document/dossier zelf (bij Wgbo, Jeugdwet of Wmo 2015 als wettelijk kader) moet worden verstrekt.
Als de AVG het wettelijk kader is, moet de beslissing een besluit zijn in de zin van de Awb. Indien de grondslag van het verzoek Wgbo of Jeugdwet betreft, dan is de beslissing een civielrechtelijke handeling binnen de contractuele relatie en is geen sprake van een besluit in de zin van de Awb.

Er werden in het afgelopen verslagjaar twee verzoeken i.h.k.v. rechten van betrokkenen onder de AVG ontvangen. Het ging om twee verwijderingsverzoeken. Het ene verzoek betreft een Regiobreed verzoek en is door omstandigheden bij verzoeker on hold gezet, het andere verzoek betreft RBL en is inmiddels afgewezen. Er werden daarnaast veel (rond tachtig) AVG-verzoeken ontvangen voor de GGD als gevolg van de datadiefstal bij GGD GHOR Nederland. Deze verzoeken zijn in het merendeel van de gevallen toegewezen.
Daarnaast werden zoals altijd meerdere inzage- en vernietigingsverzoeken bij Veilig Thuis ontvangen. Eenmaal werd een inzageverzoek bij Jeugd en Gezin ingediend. Deze verzoeken bij Veilig Thuis en

Jeugd en Gezin zijn niet onder de AVG afgehandeld maar onder de eigen materiewet, respectievelijk Wmo 2015 en Wgbo.

14 Datalekken

Een 'informatieveiligheidsincident' is een datalek indien sprake is van toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zonder dat dit de bedoeling is.
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.
Alle incidenten en datalekken moeten worden geregistreerd in het register incidenten en datalekken. Hierin staat o.a. een beschrijving van de inbreuk, de mogelijke gevolgen hiervan, de getroffen maatregelen en of hiervan een melding is gedaan aan de AP en betrokkenen.

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.

In het afgelopen verslagjaar zijn intern achtenveertig informatieveiligheidsincidenten gemeld. Dit is tweeëneenhalf keer zo veel als in het verslagjaar hiervoor. Dit kan duiden op een verhoogd bewustzijn, maar zal ook samenhangen met het feit dat voor de GGD ineens veel meer mensen zijn komen te werken ter bestrijding van corona. Bovendien waren er twee oorzaken (die inmiddels zijn weggenomen) die tot een meerdere gelijksoortige datalekken hebben geleid. Het betrof een fout in de Microsoft-software waardoor collega's documenten van anderen te zien kregen en de noodzaak een interne werkinstructie voor het checken van adressen vóór het verzenden van verwijsbrieven opnieuw onder de aandacht te brengen.
Opvallend is dat het overgrote deel van de meldingen gemaakt zijn vanaf de eerste maand van 2021, de tweede helft van het verslagjaar. Van de meldingen bleek het in vijfentwintig gevallen daadwerkelijk om een datalek te gaan. De meeste datalekken deden zich voor bij Jeugd en Gezin en GGD. Van deze vijfentwintig datalekken was in negen gevallen sprake van een risico voor betrokkenen waardoor gemeld moest worden aan de Autoriteit Persoonsgegevens. Van deze negen gevallen is vijf maal melding aan betrokkenen gemaakt, het merendeel uit zorgvuldigheid, slechts eenmaal omdat er werkelijk een hoog risico was.
De meest voorkomende datalekken vielen in de categorieën 'versturen van persoonsgegevens aan verkeerde ontvanger' en 'toegankelijkheid van persoonsgegevens voor niet-bevoegde persoon'. Het ging in het eerste geval om het versturen van brieven (vrijwel allemaal Jeugd en Gezin) of mails naar de verkeerde ontvanger. In het tweede geval ging het vaak om de hierboven genoemde Microsoft-bug waardoor mensen andermans documenten (in alle gevallen GGD-documenten) op hun bureaublad zagen staan.

15 Informatieveiligheid

Een goede inrichting van informatieveiligheid is belangrijk voor een optimale bescherming van persoonsgegevens. Er is op het gebied van informatieveiligheid echter nog behoorlijk wat (achterstallig) werk te verzetten. In het kader van de Organisatieontwikkelingsagenda zal het onderwerp 'security' als een speerpunt worden benoemd voor de komende periode.

16 Oordeel over afgelopen jaar en aandachtspunten komende periode

Het afgelopen verslagjaar lijkt het privacybewustzijn binnen de organisatie verder toegenomen. Zowel leidinggevenden als medewerkers weten de FG en de juridisch adviseurs te vinden bij vragen die verwerking van persoonsgegevens en de persoonlijke levenssfeer van betrokkene betreffen. Een belangrijke les die getrokken kan worden uit de datadiefstal bij de GGD is dat toegang tot of rechten in applicaties (en netwerkschijven) met gevoelige gegevens alleen kunnen worden verkregen indien dit noodzakelijk is om het werk te kunnen uitvoeren.
Komend jaar is het verder oppakken van de uitvoering van privacywetgeving door de RVE's van belang. De aandachtsfunctionarissen privacy spelen hierin een belangrijke rol.
Richting medewerkers zal met behulp van het afnemen van de e-learning meer aan bewustzijn worden gedaan, op het gebied van privacy maar ook op het gebied van informatieveiligheid in het algemeen.
RVE's zullen meer in de lead moeten zijn bij het (goed) afsluiten van verwerkersovereenkomsten met partijen die als een verwerker zijn aan te merken. RVE's moeten ook scherp zijn op gegevensuitwisselingen met partijen die geen verwerker van ons zijn. Hiervoor moeten mogelijk ook afspraken worden gemaakt.
Het goed invulling geven aan informatieplicht ten aanzien van verwerkingen van persoonsgegevens is komend jaar ook een belangrijk aandachtspunt voor de RVE's.

17 Aanbeveling

De FG doet een aanbeveling voor het organiseren van meer capaciteit voor het concernbreed proactief oppakken van privacygerelateerde zaken. Op dit moment is enkel de FG bestendig met proactieve privacyzaken bezig.

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.
Bovendien laat de roep om extra capaciteit zich nu meer voelen omdat op dit moment bij de overheid een professionaliseringsslag wordt gemaakt, die o.a. is ingegeven door de toeslagenaffaire, de datadiefstal bij GGD GHOR Nederland en de enorme toename van digitale dreigingen als gevolg van de coronapandemie. Deze ontwikkelingen zorgen ervoor dat ook de Regio een professionaliseringsslag dient te maken op het gebied van informatieveiligheid, maar ook op privacygebied moet verder worden geprofessionaliseerd. Dit betekent o.a. dat uitvoerende privacytaken (zoals overzetten van register van gegevensverwerkingen naar de applicatie, 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.
Ten slotte kan het beschikbaar hebben van iemand voor uitvoerende privacytaken de organisatie 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.

De hiervoor beschreven aanbeveling moet zorgen voor een betere borging van de privacy van burgers en medewerkers. De behoefte aan extra capaciteit zal in de ambtelijke organisatie worden meegenomen bij het opstellen van de nieuwe Organisatieontwikkelingsagenda.

Bijlage 1 Formele FG-adviezen

Onderwerp	Advies FG	Verwerkings-verantwoordelijke	Reactie verwerkingsverantwoordelijke
Toesturen VVV-bon voor invullen Gezondheidsmonitor V&O	Advies over het niet uitvragen van NAW-gegevens om een VVV-bon toe te sturen ter beloning voor het invullen van de verder anonieme Gezondheidsmonitor Volwassenen en Ouderen.	GGD	Gemotiveerd niet overgenomen (in de toekomst wordt dit echter niet meer zo gedaan)
Diverse beslissingen t.a.v. bestrijding van corona	Adviezen over organisatie- en systeemkeuzes bij bestrijding van corona	GGD	Wisselend
Maatregelen n.a.v. datadiefstal GGD GHOR Nederland	Advies over door GGD en FB te treffen maatregelen n.a.v. de datadiefstal bij GGD GHOR Nederland	GGD	Overgenomen
Diverse beslissingen t.a.v. verwijderverzoeken als gevolg van datadiefstal GGD GHOR Nederland.	O.a. het advies om af te wijken van landelijke lijn om gegevens van positief getesten in beginsel niet te verwijderen op verzoek.	GGD	Overgenomen
Niet gebruiken Amerikaanse internetdiensten	Advies om er voor te zorgen dat de Regio geen gebruik (meer) maakt van Amerikaanse gratis internetdiensten voor o.a. het maken van formulieren, het uitvoeren van surveys/enquêtes en het versturen van nieuwsbrieven.	Algemeen Directeur	Overgenomen
Online monitoren van inwoners	Advies aan CMT om na te gaan of de Regio gebruik maakt van nepaccounts en tooling om inwoners online te monitoren.	CMT	Overgenomen (resultaat is dat dit bij de Regio niet gebeurt)