Privacy en informatiebeveiliging

Het algemeen bestuur besprak in de vergadering van 31 maart jl. het voorstel voor de invulling van privacy en informatiebeveiliging bij GGDrU. Het algemeen bestuur constateert dat zij het onderwerp belangrijk acht. Het bestuur wil investeren in informatieveiligheid en tegelijk, gezien de financiële situatie van gemeenten, terughoudend zijn in het verhogen van de inwonerbijdrage.

GGDrU heeft niet alleen de plicht om de gezondheid van inwoners te beschermen, maar ook hun data

GGDrU werkt dagelijks met persoonlijke, gevoelige en/of vertrouwelijke (medische) gegevens, vastgelegd in vele honderdduizenden dossiers zowel in de corona- als de reguliere organisatie. De inwoner moet zekerheid hebben dat GGDrU een continue beheersing en planmatige verbetering op het gebied van informatiebeveiliging organiseert. GGDrU moet zich, net als elke andere (overheids)organisatie, daarbij houden aan de bepalingen uit de Algemene Verordening Gegevensbescherming (AVG). Zeker bij een GGD waar met (relatief veel) persoonsgegevens gewerkt wordt, is informatiebeveiliging van cruciaal belang. GGDrU heeft niet alleen de plicht om de gezondheid van inwoners te beschermen, maar ook hun data. De datadiefstal bij de landelijke organisatie laat zien hoe kwetsbaar systemen kunnen zijn. GGDrU kan nu niet soortgelijke kwetsbaarheden uitsluiten.

Informatieveiligheid moet verder ontwikkeld en geborgd worden en daarom is een degelijke en structurele invulling van informatiebeveiliging en bescherming van persoonsgegevens in de reguliere organisatie nodig. In 2019 en 2020 maakte GGDrU gebruik van een ingehuurde functionaris gegevens bescherming die tevens adviseerde over verdere invulling van informatiebeveiliging. Haar adviezen konden nog niet opgenomen worden in kaderbrief 2022 en begroting 2021 en vormen de basis voor dit huidig voorstel. Ook de concerncontroller constateert, als eigenstandig adviseur aan het bestuur, risico's in de invulling van informatiebeveiliging. Hij adviseert de het bestuur om deze te versterken. De techniek van GGDrU is in de basis op orde. Er wordt gebruik gemaakt van standaardvoorzieningen voor het beveiligen van onze systemen zoals multifactor authenticatie (MFA) en Identity- en Accesmanagement (IAM). Naast de techniek is het gedrag van mensen een belangrijke component.

In het kader van doorontwikkeling en duurzame borging van informatieveiligheid besloot het Dagelijks Bestuur een audit voor op de IT systemen (en specifiek op de status van implementatie van de AVG) van GGDrU uit te laten voeren.

Risico's

Het niet verder invullen van informatiebeveiliging brengt risico's met zich mee. Datalekken en -diefstal hebben een grote impact op inwoners. Mensen worden persoonlijk getroffen wanneer criminelen er in slagen hun persoonsgegevens te stelen. Criminelen gebruiken de gestolen gegevens namelijk voor identiteitsfraude en om spam- en phishingaanvallen uit te voeren. De schade van dergelijke oplichting kan zodanig oplopen dat
mensen echt in de problemen komen.

GGD regio Utrecht

De Autoriteit Persoonsgegevens (AP) kijkt scherp naar de informatiebeveiliging in de Zorg en kan organisaties die de AVG overtreden een boete opleggen van maximaal € 20 miljoen of 4% van de (wereldwijde) jaaromzet. Inmiddels heeft de AP al 12 boetes aan organisaties opgelegd (peildatum eind 2020). Het OLVG kreeg een boete voor slechte beveiliging van patiëntendossiers van € 440.000 en het HagaZiekenhuis van € 460.000. Recent hebben twee GGD-en (niet zijnde GGDrU) reeds een doorlichting gehad van de Autoriteit Persoonsgegevens. Op dit moment is nog niet bekend wat de (financiële) consequenties daarvan zijn.

De coronabestrijding heeft naar aanleiding van de datadiefstal bij de landelijke organisaties nog eens extra laten zien hoe actueel het thema van informatiebeveiliging is. En hoe snel het vertrouwen in de overheid geschaad wordt bij onvoldoende aandacht voor informatiebeveiliging.

Investeringen sinds 2014 via ombuigingsplan zonder verhoging inwonerbijdrage

In 2014 is reeds geconstateerd dat GGDrU kwetsbaar is op de bedrijfsondersteunende onderdelen (‘de basis’) en dat versterking van deze onderdelen noodzakelijk was voor een goede taakuitvoering. Er was een investering nodig van ruim € 1,3 miljoen. Het bestuur heeft de DPG als uitgangspunt meegegeven dat de dekking hiervoor binnen de huidige financiële kaders gevonden moest worden. Door forse inspanningen zijn de benodigde ombuigingen, zoals het nu laat aanzien, te realiseren binnen de huidige financiële kaders in de periode tot en met 2023. Vanaf 2024 resteert er dan nog een structurele ombuigingsopgave van circa €100k per jaar. GGDrU accepteert ook hiervoor de opdracht om de dekking hiervoor binnen de eigen middelen te vinden. Dit betekent dat daarmee de totale ombuiging uiteindelijk zonder een verhoging van de inwonerbijdrage gerealiseerd wordt. De inwonerbijdrage is de afgelopen jaren alleen met de reguliere indexering is verhoogd. Echter, dit betekent ook dat GGDrU (al jaren) zeer ‘scherp aan de wind’ vaart en dit ook de komende jaren zal moeten doen.

Daarnaast laat ook de laatste strategische benchmark GGDen zien dat, met een lage inwonerbijdrage vergeleken met andere GGD’en, GGDrU goede resultaten neerzet als het gaat om gezondheidsbevordering en gezondheidsbescherming.

Samenvattend kan geconcludeerd worden dat de ombuiging binnen de bestaande middelen van GGDrU kan plaatsvinden maar dat rode draad wel blijft dat er daardoor geen ruimte in de exploitatie is om tegenvallers op te vangen.

Investeringen daarom als gevolg van exogene factoren waarbij geen aanvullend budget vanuit het Rijk meekomt, zoals de invoering van de AVG, kunnen dan ook niet meer gedaan worden uit de bestaande budgetten. Deze investering kan geclassificeerd worden als ‘need-to-have’. Er ligt ook een wettelijke basis dat een overheidsinstelling de informatiebeveiliging op orde moet hebben. Anders gezegd: de investering in het op orde brengen van de invoering van de AVG is onvoorzien, onvermijdelijk en onuitstelbaar

Financiële opgaven gemeenten

Met de vraag naar aanvullende middelen beseffen bestuur en directie terdege dat de timing ervan lastig is in een tijd dat gemeenten in zwaar weer verkeren. Het algemeen bestuur stond ook in 2020 stil bij de stevige financiële opgaven voor gemeenten. Dit bestuurlijk gesprek ging over de opgaven in de publieke gezondheid, de ambities uit de bestuursagenda en de inzet van GGDrU hierin.

Het bestuur is heel tevreden met de inzet van GGD regio Utrecht, in de bestrijding van Covid-19 én in het reguliere werk in het sociaal domein; de uitvoering van wettelijke taken, collectieve taken en het maatwerk. Het bestuur wil een GGD die verantwoord zijn werk uitvoert in de minimale ruimte in wettelijke en niet wettelijke taken en is trots op de ombuigingen. Verdere bezuinigingen met de kaasschaaf zijn onmogelijk. Het bestuur zag op dit moment geen aanleiding om verder te spreken over keuzes in wettelijke en collectieve taken en vindt dat gemeenten de ruimte die het maatwerk en de afspraken over het maatwerk bieden, goed moeten benutten.

Bestuurlijke keuzes

Het algemeen bestuur besloot recent in de vergadering van 31 maart om de invulling voor het 2021 te bekostigen uit het resultaat over 2020 en daarmee tot tijdelijke dekking van de kosten. Dit betekent dat GGDrU in 2021 vooralsnog kiest voor tijdelijke versterking van privacy en informatiebeveiliging. Het algemeen bestuur besprak het voorstel voor structurele financiering in de vergadering van 31 maart jl. en kon (nog) niet tot een structureel dekkend voorstel besluiten.

Het dagelijks bestuur neemt de bespreking in het algemeen bestuur van 31 maart jl. ter harte. Zij herkennen de moeizame financiële positie voor gemeenten. Tegelijk constateren zij dat het bestuur in het najaar van 2020 besloot om GGDrU nu geen taakstelling op te leggen en dat de huidige begroting, met daarin verwerkt de inspanningen uit het ombuigingsplan, geen ruimte biedt voor de invulling van deze functies. Gezien de niet uit te sluiten majeure risico's die GGDrU loopt (en daarmee feitelijk de gemeenten) op het vlak van informatiebeveiliging ziet het dagelijks bestuur het als plicht om structurele dekking van de benodigde versterking van de AVG-maatregelen en neemt het gewogen besluit deze op te nemen in de voorliggende ontwerpbegroting. Het is een verplichting om informatiebeveiliging op een degelijke manier in te vullen.

Het Dagelijks bestuur heeft daarom in de ontwerp begroting 2022 hiervoor de benodigde bijstelling van de inwoner/kindbijdrage vanaf 2022 verwerkt. Gelezen de zienswijzen van de gemeenteraden moet de vergadering van het Algemeen Bestuur van 23 juni aanstaande blijken of hier een gekwalificeerd draagvlak voor is.

Bijlage 1: Voorstel tot invulling

AVG in control bij GGDrU? Wat hebben we nodig?

GGDrU moet zich, net als elke andere (overheids)organisatie, houden aan de bepalingen uit de Algemene Verordening Gegevensbescherming (AVG). Zeker bij een GGD waar met persoonsgegevens gewerkt wordt, is dit van cruciaal belang. In het ombuigingsplan 2020-2025 is hiervoor een eerste reservering van middelen ad €50.000 opgenomen.

Vanaf juli 2020 heeft GGDrU een Functionaris Gegevensbescherming (FG) voor 0,89 fte binnen de eigen organisatie aangesteld. Deze omvang is gekozen mede op basis van de eigen ervaringen van de afgelopen jaren maar ook om hiermee het belang van naleving van de AVG aan te geven. Voor deze invulling was het bedrag van €50.000 uit het ombuigingsplan niet toereikend. U wordt dan ook gevraagd voor een aanvullend budget voor de functie van Functionaris Gegevensbescherming €37.669.

In de jaren 2019 en deels 2020 is de functie van FG tijdelijk ingevuld door externe inhuur. Naast de reguliere werkzaamheden als FG heeft deze adviezen uitgebracht over de verdere invulling van functies ten behoeve van informatiebeveiliging. Bij dit advies zijn de praktische ervaringen van 2019 en 2020 betrokken en is een vergelijking met andere GGD'en gemaakt. Tussen GGD'en werden verschillen en overeenkomsten gezien. Verschillen in de zin dat de functies niet op dezelfde manieren worden ingevuld, overeenkomsten omdat de functies wel ingevuld worden.

Functies Privacy en Informatiebeveiliging

De functies met betrekking tot Privacy en Informatiebeveiliging in een, met de GGDrU vergelijkbare organisatie, betreffen de functies van Chief Information Privacy Officer (CISO), Privacy Officer (PO), Information Security Officer (ISO) en Contactfunctionarissen privacy en informatiebeveiliging.

Chief Security Officer (CISO)
De CISO is de eindverantwoordelijke als het gaat om de beveiliging van informatie van GGDrU. De CISO is verantwoordelijk voor het opstellen en het implementeren van het informatiebeveiligingsbeleid van GGDrU én het toezicht houden daarop door het uitvoeren van audits. De CISO heeft een centrale rol in het beheren van alle processen die daarmee te maken hebben en moet ervoor zorgen dat GGDrU voldoet aan de BIO (of NEN7510); een set van organisatorische en technische beveiligingsmaatregelen die geïmplementeerd en beheerd dient te worden.

Bij organisaties met grote hoeveelheden persoonsgegevens wordt de CISO ondersteund in zijn taak door een **Information Security Officer (ISO).** De Information Security Officer werkt vanuit kaders die door de CISO samen met de Directie worden vastgesteld. De ISO richt zich vooral op de implementatie en naleving van de kaders voor informatiebeveiliging in de operationele processen van de afdelingen. Gezien de omvang van het aantal persoonsgegevens binnen GGDrU wordt de inzet van een ISO binnen GGDrU als noodzakelijk gezien.

GGD regio Utrecht

Functionaris Gegevensbescherming (FG)
De FG is de interne toezichthouder op de naleving van de AVG en andere privacy wet- en regelgeving. Daar valt ook het toezicht op de interne verdeling van verantwoordelijkheden en de bijbehorende bewustwording of opleiding van medewerkers onder. Hij adviseert en rapporteert aan Directieteam en Bestuur. Als een Data Protection Impact Assessment (DPIA) wordt uitgevoerd, moet het advies van de FG daarbij meegenomen worden.

Privacy Officer (PO)
Waar de CISO verantwoordelijk is voor het informatiebeveiligingsbeleid is de PO verantwoordelijk voor het actualiseren en bewaken van het privacybeleid binnen GGDrU. Ten opzichte van de FG is de functie van de PO veel praktischer van aard. De PO is een operationeel uitvoerende rol en is het dagelijkse aanspreekpunt voor medewerkers wat betreft gegevensbescherming. Daar passen taken bij als adviseren over de procedures en de werkprocessen van de afdelingen, over het afsluiten van (verwerkers)overeenkomsten met externe partijen, het beheer van het verwerkingsregister en het coördineren van het proces rond datalekken. Ook is het logisch om de PO een uitvoerende rol bij het in beeld brengen van privacy risico's door middel van DPIA's te geven.

Ondanks dat er momenteel geen formele functie PO is binnen de GGDrU, worden de PO taken uitgevoerd door medewerkers binnen de organisatie; de FG neemt een aantal concrete werkzaamheden voor zijn rekening en binnen het Corona-bedrijf zijn ook medewerkers bezig met PO taken in afstemming met de FG. Daarnaast is inmiddels de capaciteit bij de GGDGHOR voor privacy en informatiebeveiliging uitgebreid, waardoor er meer ondersteuning en afstemming met de GGDGHOR mogelijk is en er bepaalde werkzaamheden binnen de GGDGHOR worden voorbereid.

De functie van CISO en ISO zijn op dit moment binnen de GGDrU niet ingevuld. De functie van CISO is, gezien de situatie rond het datalek en de reputatieschade als gevolg daarvan, het meest urgent om in te vullen. Speerpunt voor de CISO zal zijn een audit uit te voeren naar de implementatie van NEN7510 in zorginformatiesystemen.

Gefaseerde uitbreiding capaciteit

Het directieteam realiseert zich dat de invulling van alle, hierboven genoemde, functies op het gebied van privacy en informatiebeveiliging leidt tot een kostenpost en stelt daarom voor om de uitbreiding op dit gebied te faseren en de noodzaak te bezien in de ontwikkelingen het komende jaar of komende jaren.
Dit in ogenschouw nemend wordt de uitbreiding van de capaciteit gefaseerd voorgesteld.

1. **fase 1: hoogste urgentie**
   Instemmen met de uitbreiding van de capaciteit GGDrU met:
   - 0,89 fte Chief Information Security Officer (CISO), € 87.669

2. **fase 2: urgent**
   Instemmen met de uitbreiding van de capaciteit GGDrU met:
   - 1,00 fte Privacy Officer (PO), € 87.730
   - 0,50 fte Information Security Officer (ISO), € 43.865
   - Een variabele overhead € 20.000

Gevraagd budget
Om te kunnen voldoen aan de eisen van de AVG (in control zijn) voor een organisatie als en de opdracht van de GGD, conform eerdere advies van ingehuurde FG, de formatie als bovengenoemd uit te breiden.

GGD regio Utrecht

Op grond van gefaseerd voorstel, inclusief alle kosten en overhead wordt het bestuur gevraagd om uitbreiding van budget. En dit te verwerken in de begroting 2022.

- Aanvullend voor Functionaris Gegevensbescherming	€ 37.669
- 0,89 fte voor functionaris CISO	€ 87.669
- 1,00 fte voor Privacy Officer	€ 87.730
- 0,50 fte voor Information Security Officer	€ 43.865
- Variabele overhead	€ 20.000
Totale kosten	**€277.933**

Dekking van de kosten

Voor de dekking van de kosten vanaf het begrotingsjaar 2022 wordt voorgesteld om de gemeentelijke (inwoner/kind)bijdrage met dit bedrag structureel te verhogen. Op het totale volume van de begroting gaat het om een gewogen gemiddelde stijging van 0,8%. Hier zijn drie varianten voor denkbaar. Gezien de aard van de inzet van de functies ligt optie 3, een verdeling over inwoner- en kindbijdrage (40:60), voor de hand.

Drie varianten		
Optie voor dekking	Verhoging in €	Verhoging in %
1. Inwonerbijdrage	€0,204	3,5%
2. Kindbijdrage	€1,314	1,1%
3. Inwonerbijdrage / Kindbijdrage (40:60)	€0,082 / €0,791	1,4% / 0,6%

Voor de dekking van de kosten voor het begrotingsjaar 2021 wordt voorgesteld de, bij het betreffende scenario benodigde financiën, uit het verwachte positieve jaarresultaat over 2020 hiervoor beschikbaar te stellen. Hierbij kan de voorgestelde audit op IT systemen betrokken worden. In 2021 zijn de functies nog niet het gehele jaar ingevuld. Bijlage 2 geeft een overzicht van het financiële effect voor gemeenten.

GGD regio Utrecht

Bijlage 2: Kosten per gemeente

Bevolkingsaantal per gemeente per 1-1-2020				Dekkingsvoorstel Privacy en informatiebeveiliging		
Gemeente	**0 tot 18 jaar**	**18 en ouder**	**Totaal**	**IWB**	**KB**	**Totaal**
Amersfoort	34.699	122.577	157.276	€ 12.896,63	€ 27.446,91	€ 40.343,54
Baarn	4.775	20.093	24.868	€ 2.039,18	€ 3.777,03	€ 5.816,20
Bunnik	3.329	11.862	15.191	€ 1.245,66	€ 2.633,24	€ 3.878,90
Bunschoten	5.102	16.764	21.866	€ 1.793,01	€ 4.035,68	€ 5.828,69
De Bilt	8.977	34.160	43.137	€ 3.537,23	€ 7.100,81	€ 10.638,04
De Ronde Venen	8.608	35.848	44.456	€ 3.645,39	€ 6.808,93	€ 10.454,32
Eemnes	1.871	7.376	9.247	€ 758,25	€ 1.479,96	€ 2.238,22
Houten	11.789	38.357	50.146	€ 4.111,97	€ 9.325,10	€ 13.437,07
IJsselstein	7.277	26.832	34.109	€ 2.796,94	€ 5.756,11	€ 8.553,05
Leusden	6.207	24.194	30.401	€ 2.492,88	€ 4.909,74	€ 7.402,62
Lopik	3.054	11.413	14.467	€ 1.186,29	€ 2.415,71	€ 3.602,01
Montfoort	3.046	10.871	13.917	€ 1.141,19	€ 2.409,39	€ 3.550,58
Nieuwegein	11.886	51.576	63.462	€ 5.203,88	€ 9.401,83	€ 14.605,71
Oudewater	2.118	8.112	10.230	€ 838,86	€ 1.675,34	€ 2.514,20
Renswoude	1.378	4.066	5.444	€ 446,41	€ 1.090,00	€ 1.536,41
Rhenen	4.345	15.774	20.119	€ 1.649,76	€ 3.436,90	€ 5.086,65
Soest	9.313	37.293	46.606	€ 3.821,69	€ 7.366,58	€ 11.188,28
Stichtse Vecht	13.280	51.651	64.931	€ 5.324,34	€ 10.504,48	€ 15.828,82
Utrecht	70.595	287.002	357.597	€ 29.322,95		€ 29.322,95
Utrechtse Heuvelrug	9.810	39.770	49.580	€ 4.065,56	€ 7.759,71	€ 11.825,27
Veenendaal	14.812	51.681	66.493	€ 5.452,43	€ 11.716,29	€ 17.168,72
Vijfheerenlanden	11.898	44.913	56.811	€ 4.658,50	€ 9.411,32	€ 14.069,82
Wijk bij Duurstede	4.792	19.122	23.914	€ 1.960,95	€ 3.790,47	€ 5.751,42
Woerden	11.307	40.992	52.299	€ 4.288,52	€ 8.943,84	€ 13.232,36
Woudenberg	3.236	10.126	13.362	€ 1.095,68	€ 2.559,68	€ 3.655,36
Zeist	13.826	51.079	64.905	€ 5.322,21	€ 10.936,37	€ 16.258,58
Totaal regio Utrecht	**281.330**	**1.073.504**	**1.354.834**	€ 111.096,39	€ 166.691,39	€ 277.787,77

GGD regio Utrecht