GGD Hollands Noorden

Samen werken aan gezond leven

Aan	:	Dagelijks bestuur
Van	:	Edward John Paulina, Directeur Publieke Gezondheid Vanessa Kee, Manager Bedrijfsvoering
Datum	:	4 april 2023
Onderwerp	:	Noodzaak investeringen informatiebeveiliging en privacy GGD Hollands Noorden

Aanleiding

GGD HN heeft in de kadernota 2024 gevraagd om structureel extra financiële middelen, te weten € 536.000,- per jaar. Die zijn nodig ter versterking van informatiebeveiliging en privacy, met als doel de informatievoorziening voor de lange termijn te versterken en kunnen beheersen. Dit ter bevordering van de publieke gezondheid van de inwoners.

Bij de behandeling van de Kadernota 2024 in het algemeen bestuur op 15 maart 2023 is besloten de extra middelen niet toe te kennen en GGD HN opdracht te geven een voorstel te doen over de wijze waarop dit binnen de 'eigen begroting' kan worden opgelost. Dit voorstel is in de ontwerpbegroting 2024 verwerkt. Tijdens de discussie in het AB van 15 maart 2023 werd door diverse leden tevens gevraagd om een nadere onderbouwing van de kosten voor informatiebeveiliging en privacy.

De notitie is in eerste instantie besproken met de initiatiefnemer, de heer Wiesehahn. Vervolgens is de notitie op vrijdag 31 maart 2023 per e-mail onder de DB-leden verspreid voor commentaar. In overleg met de voorzitter is vervolgens besloten de notitie te agenderen voor het DB van 12 april 2023.

Hoewel het om een structurele extra bijdrage van in totaal € 536.000,- per jaar gaat, worden de totaal benodigde middelen geraamd op € 753.000,- per jaar. Bij de kadernota 2024 is reeds aangegeven dat GGD HN het verschil ad € 217.000,- als 'eigen opgave' zou oplossen. In de begroting 2024 is dan ook € 753.000,- als uitgangspunt genomen voor de voorgestelde bezuinigingen.

Hieronder volgt een nadere onderbouwing van de noodzaak voor deze structurele investering in formatie en de gevolgen bij uitblijven ervan. In deze notitie is het soms onvermijdelijk om technische termen te noemen.

Context

GGD HN speelt een cruciale rol in het beschermen en bevorderen van de publieke gezondheid en voert wettelijke en aanvullende taken uit op het gebied van publieke gezondheid. Daarvoor zijn correcte, actuele en juiste gegevens randvoorwaardelijk voor de inwoners, maar ook om de taken goed uit te kunnen voeren. De gegevens die GGD HN verwerkt zijn vaak bijzondere (medische) persoonsgegevens. Het gaat bijvoorbeeld om gegevens van kinderen, soa-uitslagen, bevindingen van lijkschouwingen, informatie rondom huiselijk geweld of data over ziekteverspreiding. Deze informatie vraagt om optimale bescherming tegen inbreuk van derden. De gevraagde financiële middelen zijn nodig om deze optimale bescherming voor de inwoners te kunnen bieden.

Historie en uitgevoerde maatregelen

Nulmeting

In 2020 is een nulmeting uitgevoerd om inzicht te krijgen in de huidige stand van zaken rondom informatiebeveiliging en privacy binnen GGD HN. Ook zijn de verschillen tussen de huidige en gewenste situatie en het bepalen van het huidige volwassenheidsniveau in kaart gebracht. Hierbij is de NEN 7510 leidend geweest, waarbij GGD HN wil streven naar volwassenheidsniveau 3. Hiermee kan GGD HN zich op termijn certificeren voor de NEN 7510. Uit de nulmeting is een volwassenheidsniveau van 1 gebleken.

NEN 7510 is een norm voor informatiebeveiliging voor de zorgsector. Het bevat technische en organisatorische voorschriften voor informatiebeveiliging gericht op het verwerken van bijzondere (medische) persoonsgegevens.

Een volwassenheidsmodel is een hulpmiddel waarin verschillende volwassenheidsniveaus zijn gedefinieerd. Hieronder worden de volwassenheidsniveaus volgens NEN 7510 weergegeven:

1	Maatregelen zijn niet aanwezig, verouderd, onvoldoende aantoonbaar, incompleet maar deels aanwezig, niet goedgekeurd of er zijn uitsluitend plannen.
2	Maatregelen zijn geïmplementeerd, maar de controle op doeltreffendheid heeft echter nog niet plaatsgevonden of de doeltreffendheid blijkt onvoldoende uit de controle.
3	Maatregelen zijn geïmplementeerd op de meest kritieke plaatsten en de doeltreffendheid is op zijn minst een keer gecontroleerd.
4	Maatregelen zijn reeds breed in de organisatie geïmplementeerd en de doeltreffendheid wordt structureel gecontroleerd.

In 2021 is een projectgroep gestart om diverse NEN 7510 maatregelen te implementeren teneinde te komen tot het gewenste volwassenheidsniveau 3. Er is een applicatie aangeschaft om medewerkers de juiste rechten in de systemen te kunnen geven en ervoor te zorgen dat medewerkers bij uitdiensttreding automatisch toegang wordt ontnomen tot de systemen van GGD HN.
Daarnaast is een applicatie aangeschaft waarmee Microsoft data van GGD HN voor een langere termijn extern worden opgeslagen.

Autoriteit Persoonsgegevens (AP)
Op 22 januari 2021 is een melding gedaan door GGD GHOR aan de AP over een datalek en de berichtgeving in de media over de handel in persoonsgegevens, afkomstig uit de systemen van de GGD'en. Hierop heeft de AP aangekondigd het toezicht op de GGD'en te intensiveren. In dit kader heeft de AP GGD GHOR en een aantal GGD'en onderzocht. Het onderzoek was gericht op het treffen van technische en organisatorische maatregelen om persoonsgegevens die verwerkt worden in het kader van testen, vaccineren en bron- en contactonderzoek passend te beveiligen. De uitkomsten uit dit onderzoek waren van toepassing op alle GGD'en.

Eén van de maatregelen vanuit de AP betrof de inrichting van een logging- en monitoringtool. Daarmee kunnen de activiteiten van zowel medewerkers als onbevoegden gemonitord worden. GGD HN heeft dit aangeschaft en de implementatie hiervan loopt. Voor het inloggen op diverse systemen is een tweeweg verificatie toegepast, wat inhoudt een extra controle op de bevoegdheid tot het inzien van gegevens.

Beveiligingstest
In 2021 heeft er binnen diverse systemen een beveiligingstest plaatsgevonden waarbij onderzocht is of deze systemen voor inbreuk van buitenaf goed genoeg afgeschermd waren. Ook werd hierbij het volwassenheidsniveau van GGD HN bepaald.

Naar aanleiding van de beveiligingstest zijn binnen de websites diverse technische maatregelen doorgevoerd, waardoor de risico's verminderd dan wel weggenomen zijn.

GGD Hollands Noorden
Samen werken aan gezond leven

Noodzaak

Wettelijk kader

Iedere GGD is geregistreerd in het Landelijk Register Zorgaanbieders (LRZA). Voor een zorgaanbieder verwijst de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) artikel 10 naar de 'Regeling gebruik Burgerservicenummer in de zorg'. In artikel 2 van deze regeling staat dat de betreffende gegevensverwerking moet voldoen aan de NEN 7510.

Binnen GGD HN worden op grote schaal bijzondere persoonsgegevens verwerkt. Op grond van artikel 32 lid 1 Algemene Verordening Gegevensbescherming (AVG) is GGD HN verplicht passende technische en organisatorische maatregelen te treffen om de gegevens van inwoners te beschermen.

Op GGD HN is eveneens de Baseline Informatiebeveiliging Overheid (BIO) van toepassing.

Deze normen vereisen van GGD HN structureel een aantal technische en organisatorische maatregelen. Te denken valt daarbij aan apparatuur en inrichting van systemen om ervoor te zorgen dat alleen bevoegden gegevens kunnen inzien. Deze middelen moeten beheerd worden, daarvoor is structureel menskracht nodig. Organisatorisch is het nodig om daarvoor processen en werkwijzen in te richten en blijvend te onderhouden via een PDCA-cyclus.

Landelijke systemen

Zowel het RIVM als GGD GHOR bieden generieke systemen aan waar GGD HN nu en in de toekomst verplicht gebruik van maakt. Voorbeelden hiervan zijn systemen rondom bron- en contactonderzoek of meldingsplichtige infectieziekten, het tuberculose register en virologische weekstaten. Beide organisaties eisen voor de toekomst dat GGD HN compliant is aan de NEN 7510. Als GGD HN niet aantoonbaar voldoet aan deze normen wordt de toegang tot deze systemen dichtgezet en heeft dit directe gevolgen voor de dienstverlening van GGD HN en vooral voor de dienstverlening aan de inwoners in het werkgebied.

Urgentie en risico's

De afgelopen twee jaar is geïnvesteerd in het op orde krijgen van de basis van informatiebeveiliging en privacy en zijn de meest belangrijke technische maatregelen getroffen. Dat is gerealiseerd met externe expertise en incidentele gelden. Nu is het urgent om dit duurzaam voor de lange termijn en intern te borgen. De huidige informatievoorziening kenmerkt zich door een grote diversiteit aan maatwerkoplossingen. De beheersbaarheid ervan staat onder grote druk en veel capaciteit van medewerkers gaat verloren aan het oplossen van incidenten. Met de huidige formatie is GGD HN niet in staat om in control te komen op de informatie-voorziening. Hierdoor blijven grote risico's bestaan ten aanzien van bedrijfscontinuïteit en informatie-beveiliging en privacy. Er is een vergroot risico op datalekken, ransomware aanvallen of phishing incidenten. Het is in het belang van de inwoners en de gemeenten om GGD HN daartegen weerbaar te maken.

Om tot het gewenste volwassenheidsniveau 3 te komen is het van essentieel belang dat de gemeenten structureel extra financiële middelen beschikbaar stellen. Als dit niet wordt toegekend blijft GGD HN op het huidige volwassenheidsniveau van informatiebeveiliging en privacy staan. De meest urgente technische maatregelen zijn getroffen waardoor de grootste kwetsbaarheden weggenomen zijn, maar het gewenste beveiligingsniveau is daarmee nog niet bereikt. Dit betekent dat werken conform de NEN 7510 niet mogelijk is. GGD HN blijft daarmee kwetsbaar voor incidenten rondom informatiebeveiliging en privacy.

Niets doen brengt risico's met zich mee. Sinds de Covid-pandemie ligt GGD HN onder een vergrootglas en worden kwaliteit en professionaliteit van GGD HN nauwlettend in de gaten gehouden. Bij nieuwe beveiligingsincidenten ontstaat onherroepelijk imagoschade voor GGD HN en de gemeenten. Het zal media aandacht genereren en bijdragen aan een verder verlies van het algeheel vertrouwen in GGD HN en de overheid.

Wat wordt er opgelost

Om te voldoen aan en blijvend te certificeren voor de NEN 7510 moet GGD HN groeien van volwassenheidsniveau 1 naar niveau 3. Volstaan met volwassenheidsniveau 1 is niet acceptabel danwel realistisch, omdat het verplichte gebruik van landelijke systemen door het RIVM en GGD GHOR afhankelijk is van de mate van informatiebeveiliging. Volwassenheidsniveau 3 is daarvoor het minimaal aangewezen niveau.

Als dat is bereikt is GGD HN in control op de informatievoorziening en zijn de grootste risico's en kwetsbaarheden op informatiebeveiliging en privacy weggenomen. Dit vereist structurele formatie omdat de informatievoorziening onderhevig blijft aan veranderingen. Capaciteit die momenteel verloren gaat aan het oplossen van incidenten kan dan blijvend worden ingezet op het voorkomen ervan. Om tot een beheersmatige situatie te komen is extra formatie nodig om dit te realiseren. Dit vraagt een inspanning van bestaande en nog aan te nemen medewerkers in de functies van:

- Privacy Officer (0,67 fte)
- Projectleider (1 fte)
- Functioneel beheerder (0,86 fte)
- Consulent DIV (1 fte)
- Data analist (0,6 fte)
- Contract- en leveranciersmanagement (0,53 fte)
- Innovatiemanager en portfoliomanagement (0,5 fte)
- Data scientist (0,2 fte)

Om hiertoe te komen is het van essentieel belang dat GGD HN de informatievoorziening meer generiek inricht met zomin mogelijk maatwerkoplossingen. Dit levert een beheersbaar informatielandschap op voor de langere termijn waarbij veiligheidsrisico's inzichtelijk zijn en incidenten kunnen worden voorkomen. Menselijke factoren zijn vaak de belangrijkste oorzaak van veiligheidsincidenten. Het vergroten van bewustwording en digitale vaardigheden van de medewerkers dragen eveneens bij aan informatiebeveiliging en privacy.

Wat is er nodig (incl. kosten)

De afgelopen jaren zijn de kosten voor de versterking van informatiebeveiliging en privacy bekostigd door het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) vanuit de zogenaamde meerkostenregeling. Deze meerkostenregeling kent een einddatum van 1 juli 2023. Vanaf dat moment dient GGD HN de kosten uit eigen middelen te bekostigen. Voor 2023 worden de kosten gedekt vanuit de algemene reserve van GGD HN. Voor 2024 en verder zal een deel van de extra kosten uit de eigen middelen van GGD worden bekostigd HN.
Voor de overige middelen en formatieve uitbreiding zijn dus geen financiële middelen beschikbaar binnen de begroting van GGD HN.

Gezien het belang en de urgentie heeft GGD HN vanaf 2022 een Functionaris Gegevensbescherming (FG), een (Chief) Informatie Security Officer (CISO en ISO) en een extra systeembeheerder bekostigd vanuit de eigen middelen.

GGD Hollands Noorden
Samen werken aan gezond leven

Om de gegevens van inwoners te beschermen is het belangrijk dat ingezet blijft worden op verdere doorontwikkeling van de informatiebeveiliging en privacy om zo te komen tot een beheersbare en veilige omgeving. De afgelopen jaren zijn diverse ICT-middelen aangeschaft en heeft formatieve uitbreiding plaatsgevonden of moet nog plaatsvinden. Vanaf 1 juli 2023 worden deze kosten niet meer gedekt vanuit de meerkostenregeling van VWS.

De totale structurele investering die van de gemeenten wordt gevraagd bedraagt totaal € 753.000,- per jaar. Een deel hiervan wordt, zoals hierboven aangegeven, structureel gefinancierd uit de eigen middelen van GGD HN, te weten € 217.000,- per jaar. Voor de overige middelen en formatieve uitbreiding zijn geen financiële middelen beschikbaar, tenzij diverse bezuinigingen binnen GGD HN worden doorgevoerd. Het kan niet anders of deze bezuinigingen zullen directe gevolgen hebben voor de dienstverlening aan de inwoners van de regio Noord-Holland-Noord.

Bij toekenning van de gelden zal halfjaarlijks gerapporteerd worden over de inzet van de middelen en de behaalde resultaten.

Onderstaand wordt een overzicht gegeven van de structurele en noodzakelijke kosten.

Overige middelen ICT beheerskosten	Noodzaak	Jaarlijkse kosten 2024
HelloID Provisioning en Service Automation	• Onderdeel van de NEN 7510 in verband met autorisatie toekenning • Zonder deze applicatie teveel handwerk, rechten en rollen worden verkeerd toebedeeld of niet ontnomen • Kans op datalekken wordt vergroot bij het niet beheersbaar inregelen van benodigde rechten en accounts	€ 14.948,–
Backit-365	• Extra beveiligingslaag tegen onopzettelijk of kwaadwillend gegevensverlies	€ 25.031,–
SOC (logging en monitoring)	• Verplichting vanuit de NEN 7510 en kans op datalekken en phishing wordt hierdoor verminderd	€ 106.876,–
Intranet vervanging	• Huidig systeem wordt niet meer ondersteund	€ 31.830,–
Password Manager	• Wettelijk vereist vanuit de NEN 7510	€ 15.915,–
Vulnerability scanning	• Noodzakelijk voor netwerkcontrole	€ 36.400,–
Totaal overige middelen ICT beheerskosten		*€ 231.000,–*
Formatieve uitbreiding	**Noodzaak**	**Jaarlijkse kosten 2024**
Privacy Officer (0,67 fte)	Wettelijk vereist vanuit AVG	€ 64.000,–
Projectleider (1fte)	Noodzakelijk ter versterking van de professionalisering van de informatievoorziening	€ 106.000,–
Functioneel beheer (0,86 fte)	Noodzakelijk in verband met business continuïteit	€ 84.000,–
Consulent DIV (1 fte)	Noodzakelijk in verband met goed beheer op documenten ten gunste van hervindbaarheid, bewaren, vernietigen en duurzame toegankelijkheid. Dit ook ter uitvoering van de Woo	€ 66.000,–
Data analist (0.6 fte)	Noodzakelijk in verband met business continuïteit	€ 71.000,–
Contract- en leveranciersmanagement (0,53 fte)	Wettelijk vereist vanuit de NEN 7510	€ 52.000.–
Innovatiemanager en portfoliomanagement (0,5 fte)	Doorontwikkeling informatievoorziening	€ 55.000,–
Data scientist (0,2 fte)	Inspelen op trends vanuit de externe omgeving ter verbetering van de dienstverlening	€ 24.000,–
Totaal Formatieve uitbreiding		*€ 522.000,–*
Totaal overige middelen en formatieve uitbreiding		**€ 753.000,–**

Specificatie te bekostigen uit eigen middelen	FTE 2024	Jaarlijkse kosten 2024
Systeembeheerder / Consulent DIV / Functionaris Gegevensbescherming	-/- 0,87	€ 74.000,-
Nog te realiseren besparing uit eigen middelen		€ 143.000,-
Totaal te bekostigen uit eigen middelen		**€ 217.000,-**

Aanvraag informatiebeveiliging en privacy	Jaarlijkse kosten 2024
Totaal overige middelen ICT beheerskosten en formatieve uitbreiding	€ 753.000,-
Totaal te bekostigen uit eigen middelen	-/- € 217.000,-
Aangevraagde verhoging deelnemersbijdrage in verband met informatiebeveiliging en privacy (€ 0,79 per inwoner)	€ 536.000,-

GGD Hollands Noorden
Samen werken aan gezond leven

Bijlage 1: Definities

Baseline Informatiebeveiliging Overheid (BIO): Opvolger van eerder gebruikte normenkaders voor de overheden, gebaseerd op de ISO 27001. Bevat technische en organisatorische voorschriften voor informatiebeveiliging voor overheidsorganen.

ISO 27001: Wereldwijd erkende norm op het gebied van informatiebeveiliging. Met een ISO 27001 certificering laat een organisatie zien dat wordt voldaan aan alle eisen rondom informatiebeveiliging.

NEN 7510: Norm voor informatiebeveiliging voor de zorgsector. Bevat technische en organisatorische voorschriften voor informatiebeveiliging gericht op het verwerken van bijzondere (medische) persoonsgegevens.

Volwassenheidsniveau: Een volwassenheidsmodel is een hulpmiddel waarin verschillende volwassenheidsniveaus zijn gedefinieerd. Hieronder worden de volwassenheidsniveaus volgens NEN 7510 weergegeven:

1	Maatregelen zijn niet aanwezig, verouderd, onvoldoende aantoonbaar, incompleet maar deels aanwezig, niet goedgekeurd of er zijn uitsluitend plannen.
2	Maatregelen zijn geïmplementeerd, maar de controle op doeltreffendheid heeft echter nog niet plaatsgevonden of de doeltreffendheid blijkt onvoldoende uit de controle.
3	Maatregelen zijn geïmplementeerd op de meest kritieke plaatsten en de doeltreffendheid is op zijn minst een keer gecontroleerd.
4	Maatregelen zijn reeds breed in de organisatie geïmplementeerd en de doeltreffendheid wordt structureel gecontroleerd.

Autoriteit Persoonsgegevens (AP): Opgericht en aangewezen als toezichthouder op de Algemene verordening gegevensbescherming (AVG) en de uitvoeringswet AVG (UAVG).

Phishing: Vorm van digitale oplichting. Hierbij misleiden criminelen organisaties met nep e-mails, nep QR-codes, valse sms- of WhatsApp berichten.

Hacking: Iemand probeert ongeoorloofd toegang te krijgen via computers of het netwerk tot de gegevens van iemand anders.

Ransomware of gijzelsoftware: Door hackers gebruikt chantagemiddel op internet.

Logging- en monitoring: Het regelmatig controleren wie wanneer toegang heeft gehad tot welke informatie.