Brabant-Zuidoost

Jaarrapportage 2024
Functionaris Gegevensbescherming

1. Inleiding

Beste lezer,

Voor u ligt de jaarrapportage van de Functionaris Gegevensbescherming van de GGD Brabant-Zuidoost over het jaar 2024. De Functionaris Gegevensbescherming is voornemens in ieder geval jaarlijks een jaarrapportage over het voorgaande jaar op te stellen. Deze frequentie kan, in overleg, worden aangepast.

Deze rapportage bevat de belangrijkste bevindingen van de Functionaris Gegevensbescherming over het afgelopen jaar, inclusief adviezen voor verbeteringen.

De Functionaris Gegevensbescherming,
Diana van Wanrooij

2. Bevindingen en adviezen

Volwassenheidsniveau

De GGD Brabant-Zuidoost heeft recent geen centraal gestuurde volwassenheidsmeting uitgevoerd om inzicht te krijgen in de volwassenheid van de organisatie op het gebied van privacy en gegevensbescherming. Het Privacy Office heeft echter de afgelopen jaren wel enkele aanzetten gedaan om te komen tot inzicht in het volwassenheidsniveau en acties om dit te verbeteren, maar dit heeft niet geleid tot structureel inzicht in het volwassenheidsniveau, een vaststelling van het beoogde volwassenheidsniveau, sturing op het volwassenheidsniveau of een structurele aanpak voor het verhogen van het volwassenheidsniveau.

Inzicht verkrijgen in het volwassenheidsniveau van GGD Brabant-Zuidoost geeft het bestuur en de directie meer inzicht in de stand van zaken van de organisatie op het gebied van privacy en gegevensbescherming. Hierdoor is er meer zicht in waar de organisatie de grootste risico's loopt, waar extra middelen benodigd zijn, en waar bijgestuurd moet worden. Daarnaast sluit het sturen op volwassenheidsniveau aan bij de aanpak van de toezichthouder, de Nederlandse Autoriteit Persoonsgegevens. De Autoriteit Persoonsgegevens heeft namelijk bij meerdere overheidsorganisaties waar zij heeft ingegrepen de verplichting opgelegd om acties te ondernemen om te komen tot volwassenheidsniveau 3 (op een schaal van 1 tot en met 5).[1]

> Advies: Gebruik het privacy volwassenheidsmodel van het Centrum Informatiebeveiliging en Privacybescherming (hierna: CIP) om meer sturing te krijgen op de AVG-volwassenheid binnen de organisatie.[2]
>
> Advies: Laat het Privacy Office een volwassenheidsmeting uitvoeren aan de hand van het volwassenheidsmodel van het CIP. Laat het Privacy Office hierover rapporteren aan, minstens, het directieniveau.
>
> Advies: Stel vast wat het beoogde volwassenheidsniveau is voor GGD Brabant-Zuidoost en stuur hierop.

Borging

Het afgelopen jaar heeft het Privacy Office een aantal wisselingen gehad in samenstelling. Dit heeft een negatieve invloed gehad op meerdere vlakken, waaronder een langere doorlooptijd van vragen in de periode dat het Privacy Office maar uit één medewerker bestond. Echter, de Functionaris Gegevensbescherming wil met name uitlichten dat dit een negatieve invloed heeft gehad op de borging van privacy en gegevensbescherming

[1] Zie hiervoor onder andere de brief van de Autoriteit Persoonsgegevens van 27 februari 2025 aan de gemeente Eindhoven en de brief van de Autoriteit Persoonsgegevens van 11 april 2024 aan de provincie Zuid-Holland.
[2] Zie: https://www.cip-overheid.nl/media/uasdokan/20171102-privacy-volwassenheidsmodel-v3_0_9.pdf

binnen GGD Brabant-Zuidoost. Voor borging moet tijd vrijgemaakt worden, voor het updaten van het verwerkingsregister en het opstellen van beleid, bijvoorbeeld, moeten uren worden vrijgemaakt. Vooral op het moment dat het Privacy Office niet volledig bezet is, krijgen ad hoc vraagstukken die betrekking hebben op lopende bedrijfsprocessen voorrang. Dat is logisch, maar met een volledige bezetting van het Privacy Office in 2025 adviseert de Functionaris Gegevensbescherming hier verandering in te brengen. Er gebeurt veel binnen GGD Brabant-Zuidoost, en veel ook op een goede manier, maar zonder gestructureerde en vastgestelde procedures en beleid wat hieraan ten grondslag ligt. Dit kan leiden tot willekeur en een onjuist toepassing van relevante wet- en regelgeving.

> Advies: Stuur erop dat er binnen het Privacy Office voldoende tijd is voor de 'borgingskant' van privacy en gegevensbescherming. Dit sluit aan bij het bovengenoemde advies over het volwassenheidsniveau. Hierbij kan gebruik gemaakt worden van jaarplannen.

Meer tijd besteden aan borging, betekent op hetzelfde moment dat er minder tijd is voor ad hoc vraagstukken over lopende bedrijfsprocessen. Hierbij is van belang dat binnen de organisatie duidelijk wordt gemaakt dat het Privacy Office, en de Functionaris Gegevensbescherming waar nodig, tijdig worden aangehaakt en dat niet verwacht kan worden dat een uitgebreide vraag binnen twee dagen beantwoord kan worden.

Een mogelijkheid hierbij is dat het Privacy Office, op basis van de volwassenheidsmeting, een plan opstelt om het volwassenheidsniveau te verhogen inclusief de tijdsinvestering die benodigd is voor de verschillende domeinen. Daarnaast houdt het Privacy Office een register bij met adviesaanvragen, waarin genoteerd wordt welke ad hoc vragen worden ontvangen, via welk kanaal deze vraag is ontvangen, hoeveel er besteed is aan de vraag en wanneer de vraag is beantwoord/afgerond. Hieruit kan worden afgelezen wat de huidige doorlooptijd is van een ad hoc vraagstuk binnen het Privacy Office. Op basis van verschillende overwegingen, inclusief het tijdspad om het volwassenheidsniveau te verhogen en wat een acceptabele wachttijd en doorlooptijd is voor ad hoc vraagstukken, kan dan een verdeling worden gemaakt in procentueel hoeveel tijd het Privacy Office besteedt aan borging, hoeveel tijd het Privacy Office besteedt aan ad hoc vraagstukken, en hoeveel tijd aan overige zaken. Het is hierbij wel van belang dat er vanuit directie en management ondersteuning is voor het Privacy Office, aangezien een cultuurverandering met een langere doorlooptijd bij het Privacy Office vaak niet direct welwillend wordt ontvangen. Het is echter wel noodzakelijk om de basis op orde te krijgen.

> Advies: Zorg ervoor dat het Privacy Office de tijd en ruimte krijgt om privacy en gegevensbescherming beter te borgen binnen de organisatie. Hierbij kan bijvoorbeeld gebruik gemaakt worden van het voorstel zoals hierboven omschreven door de Functionaris Gegevensbescherming. Zorg daarnaast ook voor voldoende rugdekking vanuit de directie en management voor het Privacy Office,

aangezien tijd en ruimte voor borging betekent dat ad hoc vraagstukken een langere doorlooptijd krijgen.

Governance

Op dit moment is niet duidelijk hoe de governance met betrekking tot privacy en gegevensbescherming precies is ingeregeld binnen GGD Brabant-Zuidoost. Een belangrijk punt hierbij is het eigenaarschap bij DPIAs: wie is er precies verantwoordelijk voor het uitvoeren van een DPIA? Wie is verantwoordelijk voor referentie DPIAs en de regionale toepassing hiervan? Wie bepaalt welke maatregelen genomen worden en welke (rest)risico's geaccepteerd worden? Wie houdt er toezicht op het implementeren van maatregelen? De onduidelijkheid over governance is niet enkel van toepassing op DPIAs, maar breder op het gebied van privacy en gegevensbescherming.

Advies: Stel een privacy governance voor GGD Brabant-Zuidoost vast.

Pilots

Binnen GGD Brabant-Zuidoost voert vaker pilots uit, vaak in samenwerking met één of enkele gemeenten binnen de gemeenschappelijke regeling. Hierbij observeert de Functionaris Gegevensbescherming dat het Privacy Office (en de CISO) vaak niet tijdig betrokken worden bij een dergelijke pilot, vaak met het argument dat bij een pilot alles nog niet juridisch goed geregeld hoeft te zijn. Dit is echter een onjuist argument, aangezien GGD Brabant-Zuidoost ook bij pilots verplicht is zich te houden aan wet- en regelgeving. Daarnaast zijn meerdere pilots uitgegroeid naar onderdeel van onze dienstencatalogus, zonder dat gegevensbescherming en informatiebeveiliging hierbij betrokken zijn.

Advies: Zorg dat het Privacy Office en de CISO vanaf het begin betrokken worden bij pilots en dat alles vanaf de start zo goed mogelijk wordt ingeregeld in lijn met geldende wet- en regelgeving. Evalueer in ieder geval bij de overgang van 'pilot' naar 'onderdeel van onze diensten' of de afspraken hierover nog steeds passend zijn bij de aangeboden diensten.

Informatievoorziening

Er zijn op dit moment drie privacyverklaringen binnen GGD Brabant-Zuidoost: een privacyverklaring voor cameratoezicht, een privacyverklaring voor sollicitanten en een algemene privacyverklaring. De algemene privacyverklaring is erg breed en het is voor betrokkenen hieruit niet op te maken wat er precies met hun persoonsgegevens gebeurt binnen de diverse diensten geboden door GGD Brabant-Zuidoost. De Functionaris Gegevensbescherming is van mening dat hier enkel sprake is van het voldoen aan de letter van de wet, namelijk aan kunnen tonen dat er informatie verschaft wordt via een privacyverklaring, en niet van voldoen aan de geest van de wet, namelijk betrokkenen inzicht verschaffen over wat er met hun persoonsgegevens gebeurt.

Advies: Stap af van één algemene privacyverklaring. Stap over op specifieke privacyverklaringen per afdeling, bijvoorbeeld een specifieke privacyverklaring voor JGZ etc. Neem hierbij ook een voorbeeld aan de privacyverklaringen op de website van de gemeente Utrecht.[3]

Tijdig betrekken Privacy Office

De Functionaris Gegevensbescherming merkt op dat het Privacy Office en/of de Functionaris Gegevensbescherming niet altijd (tijdig) betrokken worden terwijl er sprake is van zaken die zien op privacy en gegevensbescherming. Zo zijn de Functionaris Gegevensbescherming gevallen bekend waarin verzoeken werden afgewezen omdat 'het niet mag van de AVG/privacy' zonder dat het Privacy Office hierbij betrokken was, er zaken zwartgelakt worden in dossiers bij inzageverzoeken terwijl dit wettelijk niet mag zonder dat het Privacy Office betrokken is, of dat zelfs gesteld wordt dat het Privacy Office akkoord is zonder dat deze überhaupt op de hoogte is gebracht van de betreffende zaak. Dit alles kan leiden tot een onjuiste toepassing van wet- en regelgeving, stelt de GGD Brabant-Zuidoost open voor bezwaar- en beroepsprocedures, en kan een negatieve cultuur richting privacy en gegevensbescherming bevorderen.

Advies: Zorg voor voldoende bewustwording bij medewerkers dat zij weten wanneer het Privacy Office en/of de Functionaris Gegevensbescherming aangehaakt moeten worden.

Advies: Zorg voor het inbedden van het Privacy Office in huidige en toekomstige procedures die mogelijk betrekking hebben op privacy en gegevensbescherming. Neem dit tevens mee bij het vaststellen van directiebesluiten die te maken hebben met privacy- en gegevensbescherming.

Juridische zaken

De GGD Brabant-Zuidoost heeft geen afdeling Juridische Zaken. Er wordt wel gebruikt gemaakt van een externe jurist, die, waar nodig, ingeschakeld wordt. Hier zijn echter geen duidelijke richtlijnen voor en het wel of niet inzetten van de jurist brengt ook financiële overwegingen met zich mee. Het voordeel van de GGD Brabant-Zuidoost is dat over 2024 alle privacy officers en de Functionaris Gegevensbescherming juristen waren. Voor 2025 geldt, op het moment van schrijven, dat één privacy officer en de Functionaris Gegevensbescherming juristen zijn. Mochten deze personen vervangen worden, dan is de kans aanwezig dat er geen juristen meer zijn binnen de GGD Brabant-Zuidoost.

Het gebrek aan een afdeling Juridische Zaken brengt ook mee dat het Privacy Office soms zaken op moet pakken die niet bij haar takenpakket horen, zoals het beoordelen van contracten (niet enkel verwerkersovereenkomsten) en het beantwoorden van vragen op

[3] https://www.utrecht.nl/bestuur-en-organisatie/privacy/privacyverklaring

het gebied van gezondheidsrecht, zoals het doorbreken van het medisch beroepsgeheim. Op dit moment wordt dit opgepakt door de privacy officers, maar dit maakt wel een inbreuk op de tijd die nodig is voor borging en voor het behandelen van de ad hoc adviesvraagstukken. Het Privacy Office kenmerkt zich op dit onderwerp ook door verantwoordelijkheidsgevoel: er wordt gevoeld dat het niet hun taak is om dit soort zaken op te pakken, maar ze doen het toch uit verantwoordelijkheid naar de organisatie.

> Advies: Neem een jurist aan voor minstens twee dagen per week. Deze is niet enkel voor het ondersteunen van het Privacy Office bij juridische vraagstukken, maar is er juist voor de gehele organisatie. Voorbeelden hierbij zijn het ondersteunen met juridische vraagstukken bij pilots, het adviseren op het gebied van gemandateerde en gedelegeerde taken en het behandelen van bezwaar en beroep.

3. GGD GHOR Nederland

De Functionaris Gegevensbescherming sluit wekelijks aan bij het overleg met alle Functionarissen Gegevensbescherming van de 25 GGD'en inclusief de Functionaris Gegevensbescherming van GGD GHOR Nederland. Daarnaast sluit de Functionaris Gegevensbescherming, waar nodig, aan bij andere overleggen binnen de GGD GHOR Nederland structuur.

De Functionaris Gegevensbescherming wil daarnaast twee punten uitlichten over de taken die deze heeft uitgevoerd binnen de GGD GHOR Nederland structuren in 2024.

Vernieuwde datalekprocedure

De Functionaris Gegevensbescherming is betrokken geweest bij het vormgeven van de nieuwe datalekprocedure voor bovenregionale datalekken. Deze procedure ziet op datalekken die meerdere GGD'en raken.

In de vorige datalekprocedure werden alle beslissingen de facto binnen GGD GHOR Nederland genomen: het wel of niet classificeren van een incident als datalek, het wel of niet melden bij de Autoriteit Persoonsgegevens en het wel of niet informeren van betrokkenen.

Onder de vernieuwde datalekprocedure heeft de Functionaris Gegevensbescherming van GGD GHOR Nederland de verplichting om regionale Functionarissen Gegevensbescherming te consulteren en deze overwegingen mee te nemen bij het advies dat uitgebracht wordt op de bovenstaande drie beslispunten. Aangezien GGD GHOR Nederland verder weg zit van de uitvoering, zorgt deze stap ervoor dat regionale overwegingen en inzichten meegenomen worden bij het besluit. Het is aan de professionele autonomiteit van de Functionaris Gegevensbescherming van GGD GHOR Nederland om te besluiten welke regionale Functionarissen Gegevensbescherming geconsulteerd worden in een specifiek geval.

Werkgroep onderzoeksvoorstellen

GGD'en krijgen steeds vaker verzoeken van universiteiten en andere onderzoeksinstellingen om data te leveren voor (wetenschappelijk) onderzoek. In sommige gevallen gaat dit via GGD GHOR Nederland, maar in meer gevallen gaan deze verzoeken direct naar de GGD'en zelf. Het probleem is echter dat niet alle Functionarissen Gegevensbescherming evenveel kennis en ervaring hebben met wetenschappelijk onderzoek en de relevante wet- en regelgeving.

De Functionaris Gegevensbescherming van GGD Brabant-Zuidoost heeft in 2024 geopperd om een werkgroep van enkele Functionarissen Gegevensbescherming op te richten die zich meer specialiseren in het behandelen van dit soort onderzoeksvoorstellen en een referentie-advies opstellen dat overgenomen kan worden door de Functionarissen

Gegevensbescherming en GGD'en die dat willen. Vanuit de Functionarissen Gegevensbescherming is hier erg positief op gereageerd en de Functionaris Gegevensbescherming is sinds najaar 2024 de facto voorzitter van deze werkgroep.

4. Cijfers

Datalekken

In 2024 zijn er 24 datalekken geregistreerd. Dit zijn incidenten die via de officiële procedure zijn binnengekomen en die geclassificeerd zijn als datalek. Het is onduidelijk hoeveel datalekken er niet herkend zijn of die door de afdeling zelf zijn afgehandeld zonder het Privacy Office te betrekken.

Verzoeken van betrokkenen

Er zijn in 2024 42 verzoeken van betrokkenen geregistreerd bij het Privacy Office. Dit cijfer is opgebouwd uit verzoeken die rechtstreeks bij het Privacy Office zijn ingediend of waarvan JGZ het Privacy Office over geïnformeerd heeft. Het is niet duidelijk hoeveel verzoeken er door de afdelingen zijn behandeld zijn zonder het Privacy Office te informeren, met name bij JGZ en AZ, of hoeveel verzoeken er niet herkend zijn als verzoek onder de AVG.

Klachten

De Functionaris Gegevensbescherming heeft twee klachten behandeld in 2024.

DPIAs

Over 2024 zijn er vier referentie DPIAs[4] geweest waar een werkgroep van Functionarissen Gegevensbescherming een referentie advies op heeft gegeven. Een referentie DPIA is een DPIA uitgevoerd door het Privacy Office van GGD GHOR Nederland op processen die grotendeels hetzelfde zijn voor alle GGD'en.

De Functionaris Gegevensbescherming heeft geadviseerd op drie DPIAs vanuit GGD Brabant-Zuidoost.

[4] Met dit cijfer wordt enkel verwezen naar volledige DPIAs. Latere addendums, zoals bij EVS, zijn niet toegevoegd.