Jaarverslag IBP 2024

Modulaire gemeenschappelijke regeling sociaal domein Limburg-Noord (MGR)

Auteurs: mr. Kim Reijnen, Functionaris Gegevensbescherming
Jeroen Frencken, Privacy Officer

Datum: februari 2025

Inhoudsopgave

Voorwoord

Voor u ligt het Jaarverslag 2024 informatiebeveiliging en privacy (IBP) bij de Modulaire gemeenschappelijke regeling sociaal domein Limburg-Noord (MGR). In dit document geven wij de stakeholders, zoals de Directeur van de MGR en bestuursleden, inzicht in de status van de naleving van de privacywetgeving. Daarbij doen wij aanbevelingen en staan we stil bij ontwikkelingen binnen en buiten de MGR.

Inleiding

Veertien gemeenten in Noord- en Midden-Limburg (Beesel, Bergen, Gennep, Horst aan de Maas, Peel en Maas, Venlo, Venray, Weert, Nederweert, Leudal, Roerdalen, Echt- Susteren, Roermond en Maasgouw) werken samen op het gebied van inkoop van Participatie, Jeugdhulp, Wet Maatschappelijke Ondersteuning en op het gebied van Beschermd Wonen, Maatschappelijke Opvang, Bemoeizorg en Preventie. Deze gemeenten hebben een deel van de taken van het Sociaal Domein centraal belegd bij de MGR.

In beginsel is het uitgangspunt van de MGR om met geanonimiseerde gegevens te werken. Echter, bij de uitvoering van de taken kan het nodig zijn dat er toch persoonsgegevens moeten worden verwerkt. Als er persoonsgegevens worden verwerkt moet worden voldaan aan wetgeving die de bescherming van persoonsgegevens regelt. In de Algemene vordering gegevensbescherming (AVG) wordt het wettelijk kader beschreven voor de verwerking van persoonsgegevens.

Ongeacht dat het gaat om taken die bij wet aan de deelnemende gemeenten zijn toegerekend, dient de MGR zelf ook te zorgen voor de bescherming van persoonsgegevens. De MGR heeft daarnaast rechtspersoonlijkheid en draagt verantwoording voor de verwerking van de eigen persoonsgegevens binnen de organisatie, zoals de informatie over het personeel.

De functionaris gegevensbescherming (FG) houdt toezicht op de naleving van de AVG.

In dit jaarverslag informeert de FG het bestuur en directie over bevindingen met betrekking tot de wijze waarop de MGR in 2024 invulling heeft gegeven aan privacymanagement en welke werkzaamheden door de FG, de Privacy Officer (PO) en de organisatie zijn uitgevoerd in dit kader. Daarbij wordt stil gestaan bij de verplichten uit de AVG, zoals een privacybeleid en het verwerkingsregister, en worden aanbevelingen gedaan.

Terugblik en samenvatting 2024

In 2022 heeft de MGR concrete plannen gemaakt voor 2023 om de implementatie van de Algemene verordening gegevensbescherming (AVG) af te ronden. In 2023 heeft de MGR dit adequaat opgepakt en de basis op orde gebracht.

In 2024 heeft de prioriteit gelegen bij het realiseren van 'De Moderne Werkplek' in samenwerking met haar ICT-leverancier en privacymanagement. Dit laatste houdt in dat de MGR adequaat moet reageren op ontwikkelingen binnen en buiten de MGR waarbij privacy een rol speelt en aan het bewustzijn moet werken.

Verder zijn in 2024, voor zo ver noodzakelijk, de aanbevelingen uit het jaarverslag IBP 2023 opgevolgd. Hieronder een overzicht.

Aanbevelingen jaarverslag 2023	**Opgevolgd in 2024?**
In 2024 moet het privacybeleid geüpdatet worden (door de PO), getoetst (door de FG), vastgesteld en gepubliceerd. Aangezien de implementatie van de AVG is afgerond, is dit nu mogelijk.	Niet noodzakelijk gebleken, zie toelichting onder 2.
Onderzoek of de MGR een CISO (Chief Information Security Officer) moet aanstellen (of tijdelijk inschakelijken) om te voldoen aan de normen voor informatiebeveiliging.	Ja, zie toelichting onder 3.
Zorg dat duidelijk wordt of de voorzitter rol bij de MGR blijft, zodat je indien nodig contractueel de juiste afspraken kan maken met de deelnemende gemeenten en de werkwijze veilig kan inrichten.	Ja, zie toelichting onder 9.

Toelichting 2024 & aanbevelingen 2025

1. Vragen vanuit en advies aan de organisatie

Vanuit de organisatie wordt het privacyteam (FG en PO) betrokken als de medewerkers of de directeur vragen hebben over het verwerken van persoonsgegevens. We hebben in 2024 gemerkt dat medewerkers het privacyteam voor deze vragen steeds vaker weten te vinden.

De organisatie heeft verder in 2024 niet om een officieel FG-advies gevraagd en de FG heeft ook zelf geen aanleiding gezien om een ongevraagd FG-advies uit te brengen.

Generatieve AI
De MGR is aan het onderzoeken of de organisatie met Copilot kan gaan werken. In 2024 heeft de PO hier in de basis over geadviseerd. In 2025 gaat onderzocht worden of dit kan, dus of dit technisch mogelijk en ethisch verantwoord is.

<u>Aanbeveling 2025</u>
- Voor het gebruiken van AI (Copilot) moet ook onderzocht worden wat de privacy- en informatieveiligheidsrisico's zijn en hierop een risicoafweging plaatsvinden. Daarbij moet ook gekeken worden naar de verplichting "AI-geletterdheid" en wat dit betekent voor de MGR.

2. Privacybeleid

In 2024 is gekeken naar de inhoud van het privacybeleid van de MGR. De FG en PO hebben vastgesteld dat een update (nog) niet noodzakelijk was omdat de inhoud nog aansluit op de

werkelijkheid. Mogelijk waren er wijzigingen nodig na de afronding van de implementatie van de AVG, maar dit was dus niet het geval.

3. Governance

Het privacy en informatiebeveiligingsteam bestaat uit een FG en PO, voor gezamenlijk ongeveer 8 uur per week. In 2024 is dit passend gebleken.

Aanbeveling 2025
-Informatiebeveiligingsadvisering kan de PO tot op heden nog binnen zijn uren doen. Als in het derde kwartaal van 2025 de Cyberbeveiligingswet van kracht gaat of er nieuwe ontwikkelingen of ambities binnen de MGR zijn, kan het huidige aantal uren niet meer toereikend zijn. Het privacyteam zal daarover indien nodig in 2025 adviseren aan het bestuur.

4. Rechten van betrokkenen

De MGR heeft geen AVG-verzoeken van betrokkenen gehad. Dit is logisch, aangezien deze verzoeken in beginsel bij de gemeenten zelf komen. Het is wel mogelijk dat de MGR ooit een verzoek krijgt, bijvoorbeeld van een medewerker of iemand die een contactformulier op de website heeft ingevuld of dat de MGR wordt gevraagd een gemeenten te ondersteunen bij een verzoek.

5. Datalekken

Door de verplicht gestelde bewustwordingstraining voor informatiebeveiliging en privacy is ook de bewustwording t.a.v. datalekken vergroot. Dit is af te leiden uit het aantal vragen en meldingen die hierover bij de PO zijn binnengekomen.

In een aantal gevallen betrof het een naar een verkeerde ontvanger verstuurde mail. Omdat de inhoud van de mail echter geen persoonsgegevens betrof, waren deze incidenten niet te kwalificeren als een datalek. Wel is daarbij contact opgenomen met de verkeerde ontvanger om de juiste acties te ondernemen.

Slechts in één geval is er in 2024 melding gedaan van een datalek bij het privacyteam. Deze is in het register opgenomen. Dit was geen meldplichtig datalek, dus hoefde niet gemeld te worden bij de Autoriteit Persoonsgegevens (AP).

6. DPIA's

Door de MGR zijn in 2024 geen DPIA's uitgevoerd.

7. Gegevensbescherming

In oktober 2023 heeft de MGR de dienst ‘De Moderne Werkplek’ afgenomen bij de ICT-leverancier. Dit markeert een belangrijke stap in het verbeteren van de informatieveiligheid binnen de organisatie. Samen met de ICT-leverancier zijn aanvullende maatregelen getroffen. De volledige implementatie is in 2024 afgerond.

Een van de aanvullende maatregelen is de introductie van de rol Interne Administrator. Deze rol houdt toezicht op het gebruik van ‘De Moderne Werkplek’ en ondersteunt medewerkers bij vragen en beheerd de autorisaties. De Interne Administrator is verantwoordelijk voor het autoriseren van medewerkers tijdens het onboardingproces. Dit gebeurt op basis van de autorisatiematrix en rollen. Bij offboarding zorgt de Interne Administrator ervoor dat de toegangsrechten van de medewerker volledig worden ingetrokken.

Daarnaast is een beveiligingsmaatregel geïmplementeerd waarbij downloads op laptops automatisch worden verwijderd na het opnieuw opstarten van het apparaat. Hiermee voorkomen we dat documenten onnodig op laptops achterblijven.

Regionaal coördinator toegang Beschermd Wonen & Maatschappelijke Opvang
In 2024 is gebleken dat rondom deze rol de noodzaak bestond om nader te kijken naar de locatie van de opslag van eventuele persoonsgegevens die worden verwerkt bij de uitoefening van de taken. Daarom is in 2024 een afgesloten teamsomgeving voor deze rol ingericht, om ook te voorkomen dat er informatie op haar bureaublad wordt opgeslagen. Er is ook een stuk ingericht voor de communicatie met de regio, zodat informatie niet meer per mail wordt verstuurd.

Nieuwe ontwikkelingen
De nieuwe Europese Network and Information Systems Directive (NIS2-richtlijn) heeft belangrijke implicaties als het gaat om toezicht op informatieveiligheid. In tegenstelling tot de oorspronkelijkerichtlijn uit 2016 vallen lokale overheidsinstanties en dus ook de MGR nu ook onder de NIS2. Op 17 oktober is deze Europese NIS2-richtlijn in werking getreden. De lidstaten, waaronder Nederland, moesten voor deze datum de richtlijn hebben omgezet in nationale wetgeving, voor Nederland is dat de Cyberbeveiligingswet (Cbw). Nederland heeft aangegeven deze deadline niet te halen. Naar verwachting zal de Cbw in augustus 2025 in werking treden. Door de komst van de Cbw wordt ook de Baseline Informatiebeveiliging Overheid (BIO) aangepast naar de BIO2. Deze baseline wordt wettelijk verplicht via de NIS2 implementatie in de Cyberbeveiligingswet.

<u>Aanbevelingen 2025</u>

1. Voer een periodieke controle uit op het onboard- en offboardproces en de toegewezen autorisaties.
2. Stel in dat de prullenbak op laptops automatisch wordt geleegd.
3. Aangezien de BIO geldt voor Nederlandse gemeenten, en dus ook van toepassing is op de MGR, wordt aanbevolen om in 2025 te onderzoek welke invloed de bovenstaande ontwikkeling heeft op de MGR. Zie tevens de aanbeveling bij punt 3.

8. Bewustwording

In 2024 hebben alle medewerkers een trainingen over privacy & informatiebeveiliging gevolgd en een online een bijbehorend examen succesvol gemaakt. Verder zijn op het kantoor van de MGR informatie nog steeds 'bordjes’ met de 10 gouden privacy en informatiebeveiliging te vinden.

Het plan was om vanaf het tweede half jaar van 2024 periodiek een privacy en informatiebeveiliging nieuwsbrief versturen naar alle medewerkers. Aangezien medewerkers toen nog de bovenstaande trainingen moesten afronden, wordt dit meegenomen in het bewustwordingsplan voor 2025.

9. Samenwerkingen

Afspraken met de gemeente
Om regionaal te kunnen samenwerken en gegevens te verwerken is naast de reguliere overeenkomst ook een verwerkersovereenkomst nodig. Met alle deelnemende gemeenten is in 2023 de verplichte verwerkersovereenkomst afgesloten. In 2024 is dit ongewijzigd gebleven.

De GR zelf wordt geüpdatet in verband benodigde actualisatie gelet op de huidige ontwikkelingen (inhoudelijke update en doorontwikkeling van de GR zodat die aansluit op de werkelijke activiteiten en taken van de MGR). Het privacyteam blijft in 2025 betrokken bij het herschrijven zodat de benodigde afspraken over privacy en informatiebeveiliging ook hierin worden meegenomen.

In de tweede helft van 2024 is het besluit genomen dat de bijzondere toegang per 1 januari 2025 over gaat naar het Zorg en Veiligheidshuis. Per 1 januari 2025 zullen de gegevensverwerkingen niet meer bij de MGR plaatsvinden. Met het Zorg en Veiligheidshuis worden afspraken gemaakt over de data die in 2024 bij de MGR is verwerkt en het verwijderen daarvan. Financiële stromen blijven in 2025 nog wel via de MGR verlopen, maar vanaf 2025 komen er geen aanvragen meer binnen bij de MGR.

Privacy overleg
In april 2024 is een overleg georganiseerd door het privacyteam van de MGR voor de po's en fg's van de deelnemende gemeenten. Dit overleg was bedoeld om een contactmoment te creëren zodat we elkaar, waar nodig, goed weten te vinden.

Afspraken met aanbieders
De MGR is in 2024 begonnen met de acties richting de verlengingen van de overeenkomsten met aanbieders en de nieuwe inkoop met ingang van 2026. In dat kader worden in 2025 de huidige overeenkomsten geüpdatet binnen de kaders van de Aanbestedingswet en de inkoopdocumenten opgesteld voor de nieuwe inkoop.

Aanbeveling 2025
- Voeg bij de nieuwe overeenkomsten nadere afspraken in het kader van privacy en gegevensbescherming toe.

Afspraken met leveranciers
Met één leverancier is de benodigde verwerkersovereenkomst gesloten. Verder waren er geen nieuwe verwerkersovereenkomsten nodig.

10. Verwerkingsregister

In 2024 heeft het privacyteam het verwerkingsregister geactualiseerd. Daarvoor is met verschillende medewerkers gesproken, waardoor meteen is gewerkt aan de bewustwording.

Overige bevindingen 2024 en vooruitblik 2025

- Het privacyteam werkt aan een bewustwordingsplan voor 2025.
- Bij aanschaf van nieuwe applicaties/tools of ontwikkelingen rondom de GR zelf, moet in het voortraject privacy en informatiebeveiliging worden meegenomen. Dit blijft één van de hoofdonderwerpen van bewustwording binnen de MGR.
    - Vanaf 2025 gaat het privacyteam ook automatisch de verslagen van teamoverleggen (die maandelijks plaatsvinden) ontvangen, om nog sneller op de hoogte te blijven van ontwikkelingen binnen de MGR.
- De MGR heeft in 2024 het on- en off-boardingproces voor nieuwe medewerkers opgesteld en ingericht. Privacy en informatiebeveiliging wordt meegenomen in dit proces.
- Verder zal er in 2025 een periodiek overleg worden ingepland met de data analist, de officemanager, het privacyteam en indien noodzakelijk de jurist, om projecten en ontwikkelingen te bespreken.

- Einde document