Jaarverslag Informatiebeveiliging & Privacy 2022

Versiebeheer

Document:	Jaarverslag Informatiebeveiliging & Privacy 2022
Versie:	v1.0
Datum:	27-3-2023
Auteur:	Kees van Galen (FG)
Ter kennisname directie:	27-3-2023
Aangeboden aan DB:	25-5-2023

Inhoud

Inleiding

De Europese Algemene Verordening Gegevensbescherming (AVG) biedt waarborgen voor het beschermen van deze persoonsgegevens. De AVG verplicht tot het aantoonbaar treffen van beheersmaatregelen binnen organisaties om privacy en gegevensbescherming te borgen.

De Modulaire gemeenschappelijke regeling sociaal domein Centraal Gelderland (MGR SDCG) verwerkt op grote schaal persoonsgegevens van inwoners van de aangesloten gemeenten. Zonder deze gegevens kunnen de modules van MGR SDCG hun taken niet uitvoeren.

De modules Inkoop sociaal domein Centraal Gelderland (Inkoop), Contractmanagement Inburgering (CM Inburgering), Regionaal Bureau Leerlingzaken Midden-Gelre (RBL) en Werkgeversservicepunt Midden-Gelderland (WSP) voeren hun taken uit op basis van mandaat. Op basis van de AVG zijn de gemeenten de verwerkingsverantwoordelijken en is MGR SDCG de verwerker.

De module Werkgeverschap SW (WgSW) voert op basis van delegatie het werkgeverschap uit voor de SW-medewerkers die bij Scalabor BV zijn ondergebracht. Hiervoor is MGR SDCG de verwerkingsverantwoordelijke. Dat geldt ook voor het verwerken van de gegevens van medewerkers van MGR SDCG.

Naast de AVG heeft MGR SDCG ook te maken met de Wet politiegegevens (Wpg). Deze is van toepassing bij de opsporingstaken van boa’s bij RBL. Voor het verwerken van persoonsgegevens (politiegegevens) onder de Wpg is MGR SDCG zelf de verwerkingsverantwoordelijke.

In deze rapportage geeft de Functionaris voor gegevensbescherming (FG) samen met de Privacy Officer (PO) een beeld van de stand van zaken bij MGR SDCG als het gaat om het naleven van de AVG en de Wpg in 2022. De FG doet dit in zijn rol van onafhankelijke toezichthouder en brengt rechtstreeks verslag uit aan het DB.

Kees van Galen (FG/PO), maart 2023

Samenvatting en conclusie

Algemene Verordening Gegevensbescherming (AVG)

De beoordeling van de mate waarin MGR SDCG aan de AVG voldoet, visualiseren we zowel aan de hand van onderstaande symbolen, als aan de driedeling 'opzet, bestaan en werking'.

Niet onderzocht, afwezig of niet aantoonbaar	In aanzet aanwezig en aantoonbaar	Substantieel aanwezig en aantoonbaar	Grotendeels aanwezig en aantoonbaar	Volledig aanwezig en aantoonbaar	Onderzocht maar (nu) niet aan de orde.

- **Opzet**: de aanpak klopt op papier – er is goed over nagedacht.
- **Bestaan**: de aanpak is volgens plan in praktijk gebracht – MGR SDCG heeft daadwerkelijk in passende gegevensbescherming voorzien.
- **Werking**: de aanpak blijkt ook in de praktijk doelmatig en doeltreffend.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Governance	●	●	◕	Zorg voor toekomstbestendige formatie en bezetting van FG, PO (en CISO); zoek samenwerking in de regio.
Regie en support	●	◕	◕	Versterk de proactieve functie van lijnmanagers en privacy contactpersonen. Betrek de FG/PO tijdig.
Beleid	●	◕	◑	Evalueer IB- en privacybeleid en laat dit opnieuw door DB vaststellen.
Verwerkingsregister	●	●	◕	Actualiseer het register en neem ook de verwerkingen bij samenwerkingen op.
Samenwerking	●	◕	◑	Meer ketenregie. Inventariseer en analyseer de gegevensuitwisseling bij samenwerkingen.
DPIA's	●	◑	◔	Overweeg DPIA's voor bestaande verwerkingen bij actualisaties van het Verwerkingsregister.
Transparantie	●	●	●	Geen opmerkingen.
Informatiebeveiliging	●	◕	◑	Vervolg het traject van gebruik van het ISMS en neem maatregelen bij gebleken onvolkomenheden.
Datalekken	●	●	●	Geen opmerkingen.
Bewustwording	●	●	◕	Privacy-bewustzijn vergt voortdurende aandacht.
Rechten betrokkenen	●	●	●	Geen opmerkingen.

We mogen concluderen uit de bevindingen dat MGR SDCG een grote mate van aantoonbaar voldoen aan de AVG laat zien. Sinds de invoering van de AVG in 2018 is er veel werk verricht. Maar, overigens net als bij de meeste gemeenten, is er nog voldoende ruimte voor verbetering en daartoe zijn de aanbevelingen opgenomen.

De grootste uitdagingen voor 2023 zijn de governance, de ketenregie, beoordelingen en risicoanalyses van nieuwe en bestaande verwerkingen, en het uitbouwen en beter benutten van het ISMS met als doel de informatiebeveiliging beter te borgen.

Wet politiegegevens (Wpg)

Wat betreft de Wet politiegegevens (Wpg) bij de module RBL kunnen we constateren dat er in 2022 grote stappen zijn gezet om compliant te worden, om aantoonbaar aan de Wpg te voldoen. Dit blijkt zowel uit de jaarlijkse controles door de PO/FG in december, als uit het Verbeterrapport dat (als uitvloeisel van de externe audit Wpg) van februari 2023.

In 2023 zullen de nog ontbrekende maatregelen verder moeten worden ingevuld door de beleidsmedewerkers van RBL tezamen met de PO. De interne audit en de Hercontrole van de externe audit zullen eind 2023 uitsluitsel bieden over het niveau van compliancy voor alle geldende normen.

AVG aandachtsgebieden

Governance en organisatorische inbedding

MGR SDCG beschikt over een Functionaris Gegevensbescherming (FG) en een Privacy Officer (PO), die tevens fungeert als functionaris informatiebeveiliging. De PO adviseert over de naleving van de AVG en fungeert als eerste aanspreekpunt voor de organisatie. De FG is verantwoordelijk voor het toezicht op de naleving van de AVG. De rollen staan beschreven in het document MGR SDCG IB-Privacy governance.

De functie van FG is in 2022 vervuld door mr. Harmen Abbink, die van PO door drs. Kees van Galen. De heer Abbink (tevens jurist bij de gemeente Arnhem) heeft besloten zich ultimo 2022 als FG terug te trekken. Per 2023 vervult de heer Van Galen beide functies. De directie zal in de loop van 2023 met een voorstel moeten komen voor de toekomst van de governance. Daarbij wordt ook gekeken naar de wenselijkheid om de functies van FG en PO te combineren of in de toekomst weer te scheiden, en naar mogelijke samenwerkingen met andere overheidsorganen in de regio of met soortgelijke gemeenschappelijke regelingen.

De beschikbare uren voor de FG (4 upw) en PO (12 upw incl. CISO-taken) zijn krap bemeten. Dit deed zich in 2022 extra voelen door de noodzaak om de inrichting voor de Wet politiegegevens (Wpg) bij RBL op orde te krijgen. Als er discrepantie is tussen beschikbare uren en de tijd die nodig is om de wettelijke taken uit te voeren komt er druk op de verantwoordingsplicht voor de naleving van de AVG en de Wpg.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Governance	●	●	◕	Zorg voor toekomstbestendige formatie en bezetting van FG, PO (en CISO); zoek samenwerking in de regio.

Regie en support

Namens het bestuur is de directeur verantwoordelijk voor de informatiebeveiliging en privacy bij MGR SDCG. Zij wordt daarbij ondersteund door de manager bedrijfsvoering en beiden zijn het aanspreekpunt voor de FG en de PO.

Als het gaat om de uitvoering van de taken door de modules dan zijn de managers van die modules de ‘eigenaren’, ook voor informatiebeveiliging en privacy. Van hen mag een proactieve inzet worden verwacht. Bij de modules RBL en WSP (nog niet bij Inkoop) is er een ‘privacy werkgroep’, waarin IB & Privacy contactpersonen (vaak beleidsmedewerkers) samenkomen en vanuit de module actief en reactief met de PO communiceren. Het is aan te bevelen de FG en PO naar behoren en tijdig te betrekken bij alle aangelegenheden die verband houden met verwerking en bescherming van persoonsgegevens en in het bijzonder de ‘ketenregie’ te bewaken.

De PO/FG participeert in het Beveiligingsoverleg De Liemers (met de CISO’s/FG’s van Duiven, Westervoort, Zevenaar, RSD/RID en de TISO van de RID). De PO is aangemeld als ‘vertrouwde contactpersoon’ bij de landelijke Informatiebeveiligingsdienst (IBD) en ontvangt meldingen over bedreigingen.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Regie en support	●	◕	◕	Versterk de proactieve functie van lijnmanagers en privacy contactpersonen. Betrek de FG/PO tijdig.

IBP-beleid

Het privacybeleid en het informatiebeveiligingsbeleid van MGR SDCG zijn in 2018 en 2019 door het DB vastgesteld en gepubliceerd op de website. Het gaat hierbij om beleid op strategisch niveau. In grote lijnen zijn de uitgangspunten nog dezelfde. Toch is het te adviseren, zeker gezien de tijdsperiode van 4-5 jaar, het beleid opnieuw te bezien en zo nodig aan te passen en aan het DB ter vaststelling voor te leggen.

Het advies tot evaluatie en zo nodig aanpassing geldt zeker voor onderliggende beleidsplannen op tactisch niveau.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Beleid				Evalueer IB- en privacybeleid en laat dit opnieuw door DB vaststellen.

Register van verwerkingen

In het Register van Verwerkingen zijn alle verwerkingen van persoonsgegevens binnen de MGR en de modules geïnventariseerd en dit register wordt indien nodig geactualiseerd.

Waar sprake is van nieuwe verwerkingen of aanpassingen in werkprocessen dient er binnen de MGR sprake te zijn van een voortdurende dialoog tussen beleidsmedewerkers, managers/directie en de PO (en waar nodig de FG). De interpretatie is meestal geen exacte wetenschap en is vaak een afweging van wat kan en mag binnen de wettelijke kaders, en altijd vanuit het belang van en de impact op de betrokken inwoners. Waar nodig vindt er afstemming plaats met de gemeentelijke PO of FG.

Het Register van Verwerkingen voldoet aan de eisen waar het gaat om de kerntaken van de MGR en de modules. Het behoeft verbetering waar het gaat om samenwerking (en uitwisseling van persoonsgegevens) met derden.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Verwerkingsregister				Actualiseer het register en neem ook de verwerkingen bij samenwerkingen op.

Samenwerking

MGR heeft met vrijwel alle relevante partijen verwerkersovereenkomsten (vwo's) afgesloten. Dit betreft:

- Gemeenten als verwerkingsverantwoordelijke per module met MGR als verwerker. Per 2022 zijn de DVO's met de gemeenten geactualiseerd en daarmee ook de verwerkersovereenkomsten.
- MGR met subverwerkers (bv. leveranciers applicaties voor modules).
- MGR met verwerkers (zoals 1Stroom voor financiële en personeelsadministratie).
- MGR (module WgSW) met Scalabor (hybride, zowel verwerker als verantwoordelijke).
- MGR (module WSP) met UWV als met gemeenten gezamenlijke verwerkingsverantwoordelijke middels de overeenkomst UWV-portaal.

Geconstateerde omissies zijn de vwo's voor de applicatie Verdorlink bij Inkoop en met Arnhem / De Connectie voor RBL (dat huisvesting heeft in het Stadskantoor). Deze vwo's zijn nog in overleg.

De PO en FG hebben echter ook geconstateerd dat binnen de MGR de 'ketenregie' soms onvoldoende wordt bewaakt. Daarmee wordt bedoeld dat er formele of informele samenwerkingen worden aangegaan, waar niet of veel te laat de eisen betreffende privacy in beeld komen. Dit vereist proactieve ketenregie van het lijnmanagement en proceseigenaren.

De aanbeveling is om het bijhouden en interpreteren van verwerkingen beter te organiseren en de PO of FG in de beginfase te betrekken. Op korte termijn dient een inventarisatie van uitwisseling van persoonsgegevens met derden gedaan te worden. Op basis van een goede procesbeschrijving dient duidelijk te worden om welke gegevens het gaat, wie verantwoordelijk is en of voldaan wordt aan de eisen van de AVG.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Samenwerking				Meer ketenregie. Inventariseer en analyseer de gegevensuitwisseling bij samenwerkingen.

DPIA's

De AVG kent de verplichting om een risicoassessment, een DPIA (Data Protection Impact Assessment) of gegevensbeschermingseffectbeoordeling, uit te voeren voor nieuwe verwerkingen of verwerkingen met een hoog risico. Als het gaat om de kerntaken waren er het afgelopen jaar geen nieuwe verwerkingen. De module Contractbeheer inburgering valt qua werkzaamheden en systemen binnen hetgeen al gebruikelijk is bij Inkoop sociaal domein. Wel is er voor het verwerken van politiegegevens door RBL een DPIA uitgevoerd.

Het is te overwegen om periodiek ook voor bestaande verwerkingen, bijvoorbeeld bij actualisatie van het Register van Verwerkingen, een DPIA uit te voeren.

Nieuwe verwerkingen of wijzigingen van bestaande verwerkingen moeten actief en vooraf worden aangemeld bij de PO. Dat is de verantwoordelijkheid van de lijnmanager. Daarna volgt een beoordeling of een DPIA is gewenst. Dit zal ook een uitvloeisel moeten zijn van bovengenoemde inventarisatie van uitwisseling van persoonsgegevens met derden.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
DPIA's	●	◑	◔	Overweeg DPIA's voor bestaande verwerkingen bij actualisaties van het Verwerkingsregister.

Transparantie

Het recht op informatie over het verwerken van persoonsgegevens is een van de principes van de AVG. De MGR biedt die informatie in eerste instantie via de websites. Op de website van de MGR en de websites van de modules WSP, RBL en Inkoop staan de algemene en specifieke privacyverklaringen gepubliceerd. Daarin wordt o.a. uitgelegd welke persoonsgegevens we verwerken, wat de doelen zijn, wat de grondslag is voor de verwerking en dat betrokkenen het recht hebben op inzage en andere privacyrechten.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Transparantie	●	●	●	Geen opmerkingen.

Informatiebeveiliging

De Baseline Informatiebeveiliging Overheid (BIO) is ook voor de MGR het geldende normenkader. Na een eerdere GAP-analyse en een intern BIO-rapport voor het MT is in 2022 is (deels samen met partners in De Liemers) een Information Security Management System (ISMS) geïmplementeerd. Daarin is ict-dienstverlener RID De Liemers voor de MGR en de deelnemende gemeenten leidend voor de meer technische beveiligingsaspecten. Maar de MGR dient zelf de organisatorische maatregelen op orde te hebben. De controles zijn grotendeels uitgevraagd en beoordeeld, maar deels ook verschoven naar 2023, o.a. vanwege tijdsdruk en wisselingen in management bij modules. Het gebruik van het ISMS zal in 2023 een verder vervolg krijgen.

Zoals onder Governance genoemd neemt de PO van de MGR deel aan het vierwekelijkse Beveiligingsoverleg in De Liemers. Dat leidt tot gezamenlijk optrekken in uitvoeringsbeleid, bijvoorbeeld als het gaat om encryptie, autorisaties, wachtwoorden en back-ups.

Bij bedreigingen van buiten (zwaktes in systemen, meldingen van hack-pogingen elders) worden in Liemers-verband door de RID ict-technische beveiligingsmaatregelen genomen op basis van interne analyses en meldingen vanuit de IBD (Informatiebeveiligingsdienst van de VNG). Hetzelfde geldt voor De Connectie, die de ict-diensten voor RBL levert.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering

Informatiebeveiliging				Vervolg het traject van gebruik van het ISMS en neem maatregelen bij gebleken onvolkomenheden.

Datalekken

De MGR hanteert een Protocol datalekken en houdt een register bij. In 2022 was er slechts 1 inbreuk op de gegevensbescherming door de MGR (in 2021 waren het er 2). Het ging om een menselijke fout, een e-mail naar verkeerde ouder van een leerling. Het was geen ernstige incident en is meteen opgelost en niet gemeld bij de AP.

MGR constateerde wel een aantal (4x) datalekken door derden: een gemeentelijk wijkteam dat gegevens van een cliënt aan Inkoop stuurde; een bewindvoerder die een beschikking over SW-medewerkers mailde aan de MGR i.p.v. aan Scalabor en zorgverleners die gegevens cliënten aan Inkoop stuurden.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Datalekken				Geen opmerkingen.

Bewustwording

Privacy staat of valt met bewustzijn bij medewerkers. Alle medewerkers MGR doen mee aan e-learning Safe & Sound (informatieveiligheid & AVG); nieuwe medewerkers moeten deze binnen 3 maanden te hebben afgerond. Ook is er, na een pauze in de eerste helft van het jaar, in de tweede helft van 2022 een wekelijkse 'Sir Askelot' campagne Bewust in Control, met vragen die deels op maat zijn gemaakt voor de MGR. Het operationele beleid is vertaald naar 50 gedragsregels voor privacy, integriteit en informatiebeveiliging. Deze krijgen op module-niveau de nodige aandacht en vormen deel van het inwerken van nieuwe medewerkers. Daarnaast is er in de MGR Academy een aantal leerlijnen en webinars over informatiebeveiliging en privacy beschikbaar.

Via intranet zijn documenten en instructies toegankelijk voor medewerkers. Vragen die leven op de werkvloer zijn veralgemeniseerd vertaald in overzichtelijke FAQ's per module.

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Bewustwording				Privacy-bewustzijn vergt voortdurende aandacht.

Rechten van betrokkenen

De MGR hanteert een Protocol privacyrechten en houdt een register bij. Het gaat daarbij om de rechten die betrokkenen hebben op inzage, rectificatie, vergetelheid, beperking van de verwerking, bezwaar en overdracht; dit alles voor zover mogelijk binnen de wettelijke verplichtingen.

In 2022 is er geen enkele maal een beroep gedaan op deze rechten. In 2021 was dat viermaal, 4x een beroep op het inzagerecht. De verwachting dat met het ingaan van de Wet open overheid (Woo) er ook meer inzageverzoeken zouden komen is, althans bij de MGR, niet uitgekomen.

Er zijn bij de MGR geen klachten binnengekomen over de manier waarop de MGR omgaat met de privacy van betrokkenen (dat kunnen cliënten van de modules, maar ook werknemers zijn).

Speerpunt	Opzet	Bestaan	Werking	Advies ter verbetering
Rechten betrokkenen				Geen opmerkingen.

Bijhouden nieuwe ontwikkelingen

Via het Beveiligingsoverleg De Liemers is er sprake van regelmatige collegiale consultatie. FG en PO volgen algemene ontwikkelingen privacy in pers, via nieuwsberichten van de Autoriteit Persoonsgegevens en via nieuwbrieven en seminars van de IBD, VNG Realisatie en het CIP (Centrum Informatiebeveiliging en Privacybescherming). De PO participeerde in de landelijke VNG-IBD werkgroep privacyposities gemeenten en samenwerkingsverbanden.

Intensievere samenwerking in het sociaal domein

Privacybescherming wordt soms als een probleem gezien om overheidstaken goed uit te voeren. Er is een tendens om meer samen te werken in het sociaal domein. Daarbij worden de wettelijke schotten, zoals van de participatiewet, de jeugdwet en de leerplichtwet, als hinderlijk ervaren. Ook binnen de MGR leeft de wens tot overstijgende samenwerking. Een jongere die problemen heeft kan tegelijk jeugdzorg nodig hebben waarvoor een goede aanbieder ter beschikking moet zijn, als uitvallen op school en wellicht gebaat zijn met toeleiding naar werk. De insteek is dan niet legalistisch, wat volgens de AVG niet kan, maar om te onderzoeken wat wel kan en dat blijkt vaak best wel veel.

Wetgeving duurt lang en is soms fragmentarisch. Op de wet Aanpak meervoudige problematiek sociaal domein hadden zowel de AP als de Raad van State veel kritiek. Er zijn ook allerlei andere wetten in de pijplijn, bijvoorbeeld over het delen van verzuimgegevens, terugdringen verzuim, een doorbraakaanpak onderwijs en jeugdhulp, een wettelijke basis voor RMC-taken voor jongeren tussen 23 en 27 jaar, verlengde kwalificatieplicht, een wet verbetering beschikbaarheid zorg voor jeugdigen, en een wet van school naar werk. Dan doemen toch vragen op of de wens tot integrale aanpak niet zou pleiten voor integrale wetgeving, of de tendensen tot regionale aanpak niet zou pleiten voor dezelfde regio's voor verschillende wetten en in hoeverre regionale beleidsregels wenselijk zijn om te kunnen voorsorteren op komende wetten.

Digitalisering van de overheid

Binnen de overheid zien we een welhaast onstuitbare opkomst van digitale communicatie met burgers. Dat stelt toenemende eisen aan websites qua informatiebeveiliging en privacy. Maar het veronderstelt ook een digitaal bekwame burger en dat blijkt lang niet altijd het geval. Privacybescherming is ook bedoeld om de menselijke maat te blijven bewaken. Digitalisering kan burgers het gevoel geven meer als nummer dan als mens te worden gezien door de overheid.

De kwalijke zijde van digitalisering kan zich vooral doen gelden bij nieuwe technieken zoals het toepassen van algoritmes en kunstmatige intelligentie. Daarvan is bij MGR SDCG (vooralsnog) geen sprake. Maar de opmars is onmiskenbaar en de technieken bieden ook kansen, bijvoorbeeld om beter te traceren waar jongeren uitvallen in het onderwijs of om mensen aan een baan te helpen. Aan de gemeenten de uitdaging om een bestuurlijke visie op digitalisering te ontwikkelen, ook voor de taken die bij MGR SDCG zijn belegd. De AVG kan daarbij dienen als kompas om te waarborgen dat de mens, de burger van wie de gegevens worden verwerkt, centraal staat.

Wet politiegegevens

In 2021 werd bij gemeenten ten volle duidelijk dat de Wet politiegegevens (Wpg) een duidelijke afbakening met de AVG vergde. Dit was ook bij de MGR relevant vanwege de boa's werkzaam bij RBL. Voor de taken die vallen onder AVG zijn de gemeenten de verwerkingsverantwoordelijken en is MGR SDCG (waarvan RBL een module is) de verwerker. Als het gaat om taken die vallen onder de Wpg ligt dat anders, de werkgever van de boa's, dus MGR SDCG, is dan zelf de verwerkingsverantwoordelijke.

Interne en externe audit

Door de PO is in samenspraak met de manager en beleidsambtenaren van RBL een analyse gedaan. Deze inventarisatie resulteerde in een interne audit Wpg 2021. Met de (wettelijk verplichte 4-jaarlijkse) externe audit is eind 2021 aangevangen en deze is eind 2022 opgeleverd. Dat wil niet zeggen dat RBL daarop heeft gewacht. De concept audit en de gesprekken daarover hebben geleid tot diverse maatregelen ter verbetering gedurende 2022.

Jaarlijks brengen de PO en FG verslag uit aan het DB MGR SDCG (de verwerkingsverantwoordelijke voor de Wpg) over diverse aspecten betreffende de informatiebeveiliging en privacy. In het verslag over 2021 is melding gemaakt van de eerste inventarisatie en interne audit en de noodzaak van de externe audit. In het verslag over 2022 zal worden verwezen naar de externe audit, dit verbeterrapport en het vervolg.

Jaarlijks toezicht door de FG

In het (jaarlijkse) Controleplan Wpg bij RBL staat nader uitgelegd wat de toezichthoudende taken van de FG zijn en welke controles hij en de PO dienen te doen. De FG dient jaarlijks te rapporteren over de bevindingen m.b.t. de Wpg aan het DB van MGR SDCG (de verwerkingsverantwoordelijke voor de Wpg). De controles in december 2022 leverde samengevat de volgende resultaten op:

Speerpunt	Bevindingen	Advies
Beleid bescherming persoonsgegevens	In het privacybeleid wordt nog geen aandacht gegeven aan de Wpg, alleen aan de AVG.	Stel privacybeleid Wpg op en laat dit vaststellen door DB MGR SDCG. [DB heeft dit vastgesteld op 20-3-2023]
Verwerkingsregister Wpg	In het Register van verwerkingen van MGR SDCG zijn de verwerkingen die vallen onder de Wpg separaat en adequaat opgenomen. De Wpg eist ook een registratie van specifieke verwerkingen. Daartoe dient een 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens' te worden gemaakt en bijgehouden. Carel (leerlingvolgsysteem) biedt daarvoor onvoldoende mogelijkheden.	Een 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens' ontwikkelen en gebruiken. [Register VVDP is begin 2023 ontwikkeld]
Handboek Wpg / Boa-instructie	Het Handboek Wpg / Boa-instructie is in concept aanwezig. Het bestaat uit twee delen: 1. Werkinstructie voor boa's; 2. Verdieping met verwijzing naar de Wpg, geordend naar de normen en maatregelen die gehanteerd worden bij audits.	De Boa-instructie afronden en gebruik laten toetsen door de boa's. Hercontrole handboek aan de hand van Verbeterrapport Wpg bij RBL.
Autorisaties	De Wpg maakt deel uit van de MGR-brede autorisatiematrix. Deze wordt jaarlijks gecontroleerd en door het MT vastgesteld. Voor de Wpg bij RBL zijn er in 2022 ook tussentijdse controles geweest.	Documentatie en werking autorisatiebeheer in Carel.

Speerpunt	Bevindingen	Advies
Herkomst politiegegevens	In Carel wordt de herkomst van gegevens wel geregistreerd, maar niet onderscheiden naar soort verwerkingen.	Opnemen in 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens'.
Bijzondere politiegegevens	Er worden bijzondere gegevens (o.a. religieuze overtuiging, gezondheidsgegevens) verwerkt, dat is onvermijdelijk voor het doel van de verwerking, o.a. bij vrijstellingen. De gegevens zijn afdoende beveiligd in Carel volgens de TPM van de IT-auditor.	Geen opmerkingen.
Art. 9 verwerkingen	Bij RBL is geen sprake van Art. 9 verwerkingen (gerichte, uitvoerige opsporing). In Carel is geen aparte registratie mogelijk. Dus als er wel Art. 9 verwerkingen zouden komen dienen die (incl. de doelen) in een apart register te worden vermeld.	Opnemen in 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens'.
Art. 13 verwerkingen	Voor Art. 13 verwerkingen (verdere verwerkingen voor opsporing en handhaving door RBL zelf of door anderen binnen het politiedomein) dient een protocol te zijn.	Stel document 'RBL Protocollering verwerkingen art 13 Wpg' op en laat het vaststellen door DB.
Verstrekkingen aan anderen dan de politie	Werkinstructie wordt opgenomen in Handboek Wpg. Separate instructies voor vertrekkingen aan OM en Bureau Halt. Verstrekkingen aan burgemeester in Handboek Wpg. Voor verstrekkingen aan samenwerkingsverbanden (Veiligheidshuis) dient DB besluit te nemen. Verstrekkingen dienen te worden geregistreerd.	Opnemen in 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens'. DB moet besluiten dat RBL meedoet aan Veiligheidshuis en de Convenant ondertekent. OM dient ermee in te stemmen.
Aanstelling, bewustwording en opleiding Wpg	Aanstellingsprocedure, vereiste documenten, bewustwordings-activiteiten en disciplinaire procedures worden opgenomen in Handboek Wpg.	Uitwerken betreffende hoofdstukken in Handboek Wpg. Borgen werking in de praktijk.
Technische en organisatorische maatregelen	Volgens TPM Wpg Eljakim d.d. 8-12-2022 (TPM = Third Party Memorandum, verklaring door onafhankelijke IT-auditor) voldoet Carel aan alle eisen van de IT-controls en van privacy-by-design. Vrijwel alle verwerkingen bij RBL zijn art. 8 (de dagelijkse taken van de boa). Echter: Carel maakt geen onderscheid tussen de verschillende soorten verwerkingen (art. 8, 9, 11, 13) of verdere verwerkingen en is dus ook niet ingericht op de onderscheiden eisen.	RBL dient bij gesprekken met Eljakim over updates de wensen t.a.v. verbetering Carel mee te nemen. RBL moet andere dan Art. 8 verwerkingen registreren en periodiek testen of daarbij aan alle eisen wordt voldaan.
Leverancierscontract / vwo	Contract en verwerkersovereenkomst (vwo) met Eljakim dienen aan Wpg te voldoen. RBL heeft hybride verwerkersovereenkomst opgesteld, waarin MGR (voor toezicht volgens AVG) verwerker voor de gemeenten is, alsmede (voor opsporing volgens Wpg) verwerkingsverantwoordelijke. Deze vwo is op 8-12-2021 gesloten.	Toetsing van de vwo van RBL met het model dat de VNG/IBD in 2023 ter beschikking heeft gesteld.
Documentatieplicht	In MGR Register datalekken is de Wpg opgenomen. Voor zover dat niet kan in Carel dient daarbuiten aan de documentatieplicht te worden voldaan.	Een 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens' ontwikkelen en gebruiken.

Speerpunt	Bevindingen	Advies
Doelbinding	De doelbinding is afdoende opgenomen in het Handboek Wpg. De doelbinding bij art. 9, 11 e/o 13 Wpg verwerkingen en de rol van de bevoegd functionaris daarbij dient te worden geregistreerd.	Opnemen in 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens'.
Noodzakelijkheid en rechtmatigheid	Noodzakelijkheid en rechtmatigheid worden opgenomen in het Handboek Wpg. Rechtmatigheid dient bij art. 9, 11 e/o 13 Wpg verwerkingen te worden geregistreerd.	Controle Handboek Wpg. Opnemen in 'Register verwerkingen, verstrekkingen en doorgiften politiegegevens'.
Juistheid en volledigheid	Juistheid en volledigheid zijn opgenomen in het Handboek Wpg. Door RBL worden er geen systematische controles gehouden. Wel vinden er extra controles op integriteit plaats als er sprake is van een grote caseload bij medewerkers en bij startende medewerkers. In Carel is de integriteit van gegevens door een BRP- en BAG-koppeling gewaarborgd. Vernietiging is in Carel ingericht volgens de eisen bij Art. 8 verwerkingen.	Zorg voor procedure voor en planning van controles en maak verslagen. Maak RBL-procedure voor het vernietigen van politiegegevens.
Onderscheid feiten en meningen	Onderscheid feiten en meningen is opgenomen in het Handboek Wpg. In Carel is er ruimte voor dit onderscheid in de dossiers. Sjablonen voor verslagen moeten nog worden aangepast.	RBL dient z.s.m. in de sjablonen voor verslagen en verhoren onderscheid te maken tussen feiten en meningen.
DPIA's	PO heeft met behulp van de IRPA-tool (van de VNG/IBD) eind 2021 een DPIA uitgevoerd. De externe auditor vond deze onvoldoende en te weinig op de Wpg gericht.	Actualiseren DPIA.
Logbestanden	Ten tijde van de controle waren de logbestanden niet beschikbaar. RBL zal deze bij Eljakim opvragen zodat ze alsnog gecontroleerd kunnen worden.	Controle logbestanden.
Audits	Voorafgaande aan de externe audit is er een interne audit 2021 gedaan, gebaseerd op het VNG-model. De bevindingen daarvan zijn door de externe auditor geadresseerd in zijn audit over de periode t/m 30-11-2021, die op 18-11-2022 is opgeleverd, besproken door het DB van MGR SDCG en is vertrekt aan de Autoriteit Persoonsgegevens (AP). Er is een Auditplan Wpg bij RBL opgesteld, met daarin de randvoorwaarden van de interne audits, de planning en de reikwijdte.	Actualisatie Auditplan Wpg bij RBL voor interne audit 2022.
Toezichttaken FG	De wettelijk verplichte toezichttaken (het naleven van de Wpg; het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens; de toewijzing van de autorisaties, bedoeld in art 6; de bewustmaking en opleiding van de boa's en andere functionarissen die betrokken zijn bij de verwerking van politiegegevens; de audits; en de uitvoering van de DPIA's) worden hierboven geadresseerd.	Laten terugkomen in RBL Controleplan Wpg 2023.

Speerpunt	Bevindingen	Advies
	Wat betreft de toewijzing van de autorisaties heeft RBL gekozen voor het door het DB van MGR SDCG op 11-10-2021 laten aanwijzen van één Bevoegd Functionaris, in casu de manager RBL. Daarmee is deze gemachtigd om daar waar in de Wpg sprake is van een bevoegd functionaris (i.h.b. bij art 9, 11 en 13 verwerkingen) deze functie te vervullen.	
Verslag aan DB	De eis is: de FG stelt jaarlijks een verslag op van zijn bevindingen en stelt het ter beschikking aan de verwerkingsverantwoordelijke. In 2022 is door de PO, mede namens de FG, de Wpg kort toegelicht in het Verslag stavaza informatiebeveiliging, privacy & archiefbeheer. Op 18-11-2022 stond de externe audit Wpg op de agenda van het DB.	Jaarverslag 2022 met daarin zowel IBP (Informatiebeveiliging & Privacy) als Wpg. Hierbij!

Verbeterrapport en hercontrole

De wet verplicht dat er drie maanden na de externe audit (d.d. 18-11-2022) een verbeterrapport moet worden gemaakt. De controleperiode van de audit liep t/m 30-11-2021. Dus het verbeterrapport omvat de maatregelen die sinds die datum al dan niet zijn getroffen. Het RBL Verbeterrapport Audit Wpg (d.d. 17-2-2023) is dan ook een aanvulling op dit toezichtverslag en geeft een overzicht van alle maatregelen en alle normen voor de Wpg. In een uitgebreid overzicht wordt aangegeven welke maatregelen dan wel ‘gereed’, ‘in behandeling’, of nog in de ‘beginfase’ zijn.

In 2023 zal er een interne audit Wpg 2022 worden gedaan. Uiterlijk een jaar na de externe audit (dus uiterlijk 18-11-2023) dient er een hercontrole plaats te vinden van die externe audit. Dat betekent dat RBL, samen met de PO, tot die datum er werk van zal maken om zo veel mogelijk maatregelen de status van ‘gereed’ te laten bereiken.

Lijst van begrippen en afkortingen

1Stroom	werkorganisatie voor de gemeenten Duiven en Westervoort
AVG	Algemene Verordening Gegevensbescherming
AP	Autoriteit Persoonsgegevens
BIO	Baseline Informatiebeveiliging Overheid
boa	buitengewoon opsporingsambtenaar
Carel	applicatie van Eljakim BV, die door RBL wordt gebruikt om leerlingen te volgen
CIP	Centrum Informatiebeveiliging en Privacybescherming
CISO	Chief Information Security Officer
CM Inburgering	module Contractmanagement Inburgering
datalek	inbreuk op de gegevensbescherming waarbij data zijn gelekt of hadden kunnen lekken
De Connectie	Ict-dienst voor de gemeenten Arnhem, Renkum en Rheden
DPIA	Data Protection Impact Assessment), gegevensbeschermingseffectbeoordeling
FAQ	Frequently Asked Questions
FG	Functionaris Gegevensbescherming
IBD	Informatiebeveiligingsdienst (van de VNG)
IBP	Informatiebeveiliging en Privacy
ict	informatie- en communicatietechnologie
Inkoop	module Inkoop sociaal domein Centraal Gelderland
IRPA	Integrale Risico en Privacy Analyse tool van de IBD
ISMS	Information Security Management System
IT-auditor	information technology auditor, die oordeelt en adviseert over IT in bedrijven en organisaties
IT-controls	information technology controls, beheersmaatregelen die een organisatie heeft getroffen om ervoor te zorgen dat de IT-systemen betrouwbaar en integer zijn
MGR / MGR SDCG	Modulaire gemeenschappelijke regeling sociaal domein Centraal Gelderland
MT	Management Team van MGR SDCG
OM	Openbaar Ministerie
PO	Privacy Officer
RBL	module Regionaal Bureau Leerlingzaken Midden-Gelre
RID	RID De Liemers, ict-dienst voor de gemeenten Duiven, Westervoort en Zevenaar en voor de RSD en MGR SDCG.
RSD	RSD De Liemers, Regionale Sociale Dienst voor de gemeenten Duiven, Westervoort en Zevenaar
TISO	Technical Information Security Officer
TPM	Third Party Memorandum, verklaring van onafhankelijke audit partij over de kwaliteit van een ICT-dienstverlening en -beheersing van een organisatie
Veiligheidshuis	regionaal samenwerkingsverband waarin verschillende instellingen werken aan het terugdringen van overlast, huiselijk geweld en criminaliteit
VNG	Vereniging van Nederlandse Gemeenten
vwo	verwerkersovereenkomst
WgSW	module Werkgeverschap SW
WOO	Wet open overheid
Wpg	Wet politiegegevens
WSP	module Werkgeversservicepunt Midden-Gelderland