Verslag Informatiebeveiliging & Privacy

Governance en organisatorische inbedding

MGR SDCG beschikt over een Functionaris Gegevensbescherming (FG) en een Privacy Officer (PO), die tevens fungeert als functionaris informatiebeveiliging (en functionaris archief en klachtencoördinator). De rollen staan beschreven in het document MGR SDCG IB-Privacy governance. De managers van de modules zijn de 'eigenaren'. Per module zijn er IB & Privacy contactpersonen (vaak beleidsmedewerkers).
De PO participeert in het Beveiligingsoverleg De Liemers (met de CISO's/FG's van Duiven, Westervoort, Zevenaar, 1Stroom en de CISO en TISO van de RID). De PO is aangemeld als 'vertrouwde contactpersoon' bij de landelijke Informatiebeveiligingsdienst (IBD) en ontvangt meldingen over bedreigingen.

IBP-beleid

Het privacybeleid en het informatiebeveiligingsbeleid van MGR SDCG zijn in 2018 en 2019 door het DB vastgesteld en gepubliceerd op de website.

Privacyverklaringen

Op de websites van de MGR en van de modules WSP, RBL en Inkoop staan de algemene en specifieke privacyverklaringen gepubliceerd.

Privacyrechten

De MGR hanteert een Protocol privacyrechten en houdt een register bij. In 2020 is er tweemaal een beroep op het inzagerecht gedaan, 1x bij RBL, 1x bij Inkoop. In beide gevallen speelde er ook andere problematiek en was het beroep op recht van inzage deel van de afhandeling van een conflict. In beide gevallen zijn ze afgehandeld in overleg met de (verwerkingsverantwoordelijke) gemeente.

BIO – norm voor informatiebeveiliging

Sinds 2020 geldt de Baseline Informatiebeveiliging Overheid (BIO) voor gemeenten en verlengde overheden zoals de MGR. Op basis van de GAP-analyse van de Informatiebeveiligingsdienst (IBD) is MGR-breed (en voor de technische kant via de ict-dienstverleners RID De Liemers en De Connectie) gedurende 2020 een inventarisatie gemaakt. Dat heeft geresulteerd in een BIO-rapport waarmee het MT eind 2020 de stand van zaken in kaart heeft gebracht. In 2021 worden maatregelen genomen voor verdere verbeteringen.
In Liemers-verband worden door de RID ict-technische beveiligingsmaatregelen genomen op basis van interne analyses en meldingen (zoals de Citrix-crisis begin 2020 en de Hof van Twente-hack eind 2020).

Datalekken

De MGR hanteert een Protocol datalekken en houdt een register bij. In 2020 waren er 3 inbreuken op de gegevensbescherming bij de MGR. 1x de diefstal van een laptop (data op afstand gewist). 1x niet afdoende segmentering op intranet, waardoor gegevens zichtbaar waren voor enkele niet geautoriseerde beheerders. 1x mail naar verkeerd adres bij RBL. Het waren geen ernstige incidenten en ze zijn meteen opgelost.
MGR constateerde wel een aantal datalekken door derden, enkele keren zorgaanbieders die gegevens aan Inkoop stuurden i.p.v. aan de gemeenten, en bewindvoerders die beschikkingen over SW-medewerkers stuurden aan de MGR i.p.v. aan Scalabor. Ze werden veroorzaakt door de voor derden soms als complex ervaren structuur van de MGR en het waren er duidelijk minder dan in 2019.

Bewustwording en inbedding

Alle medewerkers MGR doen mee aan e-learning Safe & Sound (informatieveiligheid & AVG) en de wekelijkse campagne Bewust in Control. 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 worden veralgemeniseerd vertaald in overzichtelijke FAQ's per module.

Bijhouden en interpreteren van verwerkingen

In het Register van Verwerkingen zijn alle verwerkingen van persoonsgegevens binnen de MGR en de vier modules geïnventariseerd en dit register wordt indien nodig geactualiseerd.
Waar sprake is van nieuwe verwerkingen of aanpassingen in werkprocessen is er binnen de MGR sprake 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.

Samenwerking

MGR heeft met alle relevante partijen verwerkersovereenkomsten afgesloten. Dit betreft:

- Gemeenten als verwerkingsverantwoordelijke per module met MGR als verwerker.
- 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.

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 seminars van de IBD, VNG Realisatie en het CIP (Centrum Informatiebeveiliging en Privacybescherming).
De PO participeert in de landelijke IBD werkgroep privacyposities gemeenten en samenwerkingsverbanden.
De MGR kan gebruikmaken van een information security management system (ISMS), dat steeds wordt geactualiseerd. Het huidige systeem wordt uitgefaseerd en binnen De Liemers zal een nieuw ISMS worden aangeschaft, volgens de nu geldende eisen en volgens een nader vast te stellen verdeelsleutel.

Verslag d.d. 31-5-2021 door Kees van Galen (PO)