Rekenkamer Rijswijk

PRIVACY IN HET SOCIAAL DOMEIN

BESTUURLIJKE NOTA

Rekenkamer Rijswijk

Aanleiding

Privacy en de bescherming van persoonsgegevens is een belangrijk thema binnen gemeenten. Er wordt veel gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Daarnaast is het thema blijvend relevant vanwege nieuwe technologische ontwikkelingen en een steeds meer digitale overheid. De bescherming van persoonsgegevens is onderdeel van een integere dienstverlening en de burger moet erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met persoonsgegevens omgaat. Dat geldt voor alle inwoners van Rijswijk, maar zeker voor de kwetsbare inwoners van de gemeente. Daarom heeft de Rekenkamer Rijswijk besloten dit onderzoek ter hand te nemen.

Voor u liggen de conclusies en aanbevelingen die de Rekenkamer Rijswijk heeft opgesteld naar aanleiding van het onderzoek naar privacy en informatieveiligheid in het sociaal domein. De Rekenkamer heeft onderzocht hoe invulling wordt gegeven aan de borging van privacy en de bescherming van persoonsgegevens in het sociaal domein van de gemeente Rijswijk.

Voor dit onderzoek stond de volgende onderzoeksvraag centraal:

In hoeverre is de privacy van inwoners en de beveiliging van persoonsgegevens in het sociaal domein van de gemeente Rijswijk gewaarborgd?

Voor de beantwoording van deze vraag heeft de Rekenkamer onderzoeksbureau Unravelling in de arm genomen. Hun onderzoeksbevindingen zijn terug te vinden in de bijgesloten nota van bevindingen.

I. Conclusies

Op basis van het uitgevoerde onderzoek komt de Rekenkamer tot de volgende conclusies:

1. Het privacybeleid van de gemeente is in lijn met de AVG, maar er zijn verbeterpunten

Het privacybeleid van de gemeente is in lijn met de AVG, maar de gemeente heeft de normen uit de AVG herhaald en niet nader geconcretiseerd. Dit is volgens de Autoriteit Persoonsgegevens niet voldoende. Ook de privacyprocessen zijn op hoofdlijnen in orde, maar kunnen verbeterd worden op de volgende punten:

- De gemeente voert geen risicoanalyses (DPIA's) uit op bestaande processen;
- Autorisaties zijn niet altijd navolgbaar;
- Er wordt niet altijd rekening gehouden met de beginselen van Privacy by Design en Privacy by Default;
- Het loggingsbeleid is niet volledig op orde.

2. Het beheer van datalekken is op orde, maar de meldingsbereidheid is een aandachtspunt, evenals opleiding en training

De gemeente houdt een register van datalekken bij en heeft het beheer van datalekken op orde. Er worden echter vrijwel geen van de geconstateerde datalekken bij de Autoriteit Persoonsgegevens gemeld.. De gemeente Rijswijk meldt beduidend minder datalekken dan andere gemeenten, terwijl het aantal datalekken wel vergelijkbaar is.

De gemeente besteedt aandacht aan het bewustzijn van (nieuwe) medewerkers om eventuele schaamte voor het melden van datalekken te minimaliseren. Het lijnmanagement wijst (externe) medewerkers echter niet voldoende op de beschikbaarheid en het nut van opleidingen en trainingen op het vlak van privacy.

3. De gemeentelijke website bevat voldoende informatie over privacy

De gemeentelijke website bevat voldoende informatie voor inwoners, zoals over privacy, de rechten van betrokkenen en het melden van datalekken.

4. **Consulenten zijn transparant naar burgers over de verwerking van hun gegevens, maar het uitsluitend werken met mondelinge toestemming vormt een risico**

Over het algemeen informeren consulenten burgers en nemen zij hen mee in wat zij doen met hun gegevens. Bij het Jeugdteam wordt met mondelinge toestemming voor het verwerken van iemands persoonsgegevens gewerkt in plaats van een schriftelijke, waardoor de registratie daarvan tekortschiet en de toestemming niet navolgbaar is. Dit vormt een juridisch risico voor de gemeente. Bovendien kunnen burgers achteraf niet nalezen waarmee ze precies ingestemd hebben.

5. **De gemeente heeft inzichtelijk welke risico's er momenteel op het gebied van informatiebeveiliging bestaan, maar het bewustzijn over de noodzaak en vanzelfsprekendheid van acties om risico's zoveel mogelijk te beperken, is een verbeterpunt**

Risico's zijn onder andere wachtwoordvereisten, twee factorauthenticatie, de functieautorisatiematrix en het beveiligd communiceren met inwoners. In het kader van leren en verbeteren is het van belang dat er zicht is op de mate waarin leidinggevenden incidenten en verbeterpunten oppakken. Op dit moment is dat onvoldoende het geval.

6. **De rol van de raad bij het privacy- en informatiebeveiligingsbeleid is beperkt**

De gemeenteraad van Rijswijk is betrokken geweest bij de ontwikkeling van het informatiebeleidsplan, maar in beperkte mate. Het borgen van privacy- en informatiebeveiligingsbeleid wordt gezien als een bedrijfsvoeringskwestie. Enerzijds mag de raad verwachten dat het college de borging goed organiseert. Anderzijds, moet de raad hier ook zelf op toezien. Daarnaast neemt het college de raad weinig mee in het thema privacy en informatieveiligheid, waardoor de raad niet in staat wordt gesteld om te sturen en controleren op dit thema.

II. Aanbevelingen

De Rekenkamer Rijswijk formuleert op basis van bovenstaande conclusies de volgende vier aanbevelingen.

1. **Geef meer aandacht aan opleiding en training van (externe) medewerkers in het sociaal domein op het vlak van privacy**

In het sociale domein worden dikwijls gevoelige persoonsgegevens verwerkt. Opleiding en training op het vlak van privacy van medewerkers is essentieel om zorgvuldig met persoonsgegevens om te kunnen gaan, volgens de vereisten die de AVG voorschrijft. Besteed hier (nog) meer aandacht aan en heb daarbij specifiek oog voor externe medewerkers.

2. **Monitor als college op welke wijze het lijnmanagement verbeterpunten oppakt**

Op dit moment is er onvoldoende zicht op de mate waarin leidinggevenden incidenten en verbeterpunten oppakken, terwijl dit wel van wezenlijk belang is in het kader van leren en verbeteren. We bevelen aan dat de Functionaris Gegevensbescherming dit als onderdeel van zijn jaarverslag monitort en hierover rapporteert.

3. **Voer op basis van dit onderzoek een aantal verbeterpunten uit om de privacy van inwoners nog beter te borgen**

Het college kan met een aantal concrete verbeterpunten de privacy van de inwoners beter borgen. Daarbij gaat het bijvoorbeeld om het schriftelijk vastleggen van (mondelinge) toestemming voor het gebruik van persoonsgegevens, het gebruiksvriendelijk, beveiligd communiceren met burgers en het verbeteren van de organisatie brede functie-autorisatiematrix. Het is aan de Functionaris

Gegevensbescherming (FG) en de Chief Information Security Officer (CISO) om te blijven monitoren of dergelijke verbeterpunten opgepakt worden.

4. Versterk de rol van de raad bij het privacy- en informatiebeveiligingsbeleid

Het college en de raad hebben elkaar nodig om kaders te stellen op het vlak van privacy- en informatiebeveiliging, zodat de raad het college goed kan sturen en controleren. De raad moet hierbij actiever toezien op de borging van deze onderwerpen, in plaats van vooral incidentgericht te reageren. Privacy is immers meer dan alleen een bedrijfsvoeringsaangelegenheid. Hiervoor is het nodig dat het college de raad actief meeneemt in de thema's privacy en informatieveiligheid, zodat de raad ook daadwerkelijk zijn controlerende en toezichthoudende rol kan vervullen en erop kan toezien dat privacybescherming goed geborgd is.