Rekenkameronderzoek gemeente Rijswijk

Privacy en informatieveiligheid in het sociaal domein

Rekenkamer Rijswijk

18 november 2021

Martijn Mussche
Shauni Drost

Inhoud

Inhoudsopgave

Afkortingen en begrippenlijst

Begrip en afkorting	Uitleg
Autorisatiematrix	In een autorisatiematrix is zichtbaar wie binnen de organisatie welke rechten heeft (inzien, bewerken etc.). en voor welke persoonsgegevens die rechten gelden. De matrix legt dus vast wie bij welke gegevens kan en waarom.
Autoriteit Persoonsgegevens (AP)	De toezichthouder op het gebied van privacywetgeving.
Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG)	Voorloper van de BIO.
Baseline Informatiebeveiliging Overheid (BIO)	De BIO is een normenkader voor informatiebeveiliging en geeft het basisniveau voor informatiebeveiliging waar alle overheidspartijen aan moeten voldoen. Het is gebaseerd op de actuele, internationale standaarden voor informatiebeveiliging, de ISO 27001 en 27002.
BIO-SA (Self-Assessment)	De BIO-SA is een krachtig doe-het-zelf instrument om te meten hoe volwassen de organisatie omgaat met informatiebeveiliging. Het is ook een stuurinstrument voor stapsgewijze planmatige verbetering en een krachtig middel voor het vergroten van bewustwording bij management en medewerkers.
Borgingsproduct	Het borgingsproduct is een instrument dat gemeenten handvatten geeft om een goede omgang met persoonsgegevens binnen de gehele gemeente te waarborgen. De gemeente kan met het borgingsproduct een ambitieniveau bepalen en laten vaststellen. De proceseigenaren kunnen, met ondersteuning van bijvoorbeeld de privacyofficer, het borgingsproduct gebruiken om periodiek te toetsen waar de gemeente staat.
Chief Information Security Officer (CISO)	De CISO is verantwoordelijk voor de implementatie van het informatiebeveiligingsbeleid en het toezicht op de uitvoering ervan.
Datalek	Iedere inbreuk op de beveiliging waarbij persoonsgegevens verloren zijn gegaan of ongeoorloofd zijn gewijzigd, verstrekt of ingezien.
Data protection impact assessment (DPIA)	Onder de Algemene verordening gegevensbescherming (AVG), de Wet politiegegevens (Wpg) en de Wet justitiële en strafvorderlijke gegevens (Wjsg) kunnen organisaties verplicht zijn een data protection impact assessment (DPIA) uit te voeren. Dat is een instrument om vooraf de privacyrisico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen. Het is verplicht wanneer een gegevensverwerking waarschijnlijk een hoog privacyrisico oplevert voor de mensen van wie de organisatie gegevens verwerkt. Dit moet de verwerkingsverantwoordelijke zelf bepalen. U mag in dat geval niet beginnen met het verwerken van gegevens voordat u een DPIA (en indien nodig een voorafgaande raadpleging) heeft uitgevoerd.
Eenduidige Normatiek Single Information Audit (ENSIA)	ENSIA is een gezamenlijk initiatief van de ministeries Binnenlandse Zaken en Koninkrijksrelaties, (voormalig) ministerie van Infrastructuur

	en Milieu, Sociale Zaken en Werkgelegenheid en de Vereniging van Nederlandse Gemeenten (VNG) om te komen tot een zo effectief en efficiënt mogelijk verantwoordingsstelsel voor informatieveiligheid. Het is per 1 juli 2017 geïmplementeerd.
Functionaris gegevensbescherming[1] (FG)	De FG is de interne toezichthouder op de naleving van de AVG binnen de organisatie.
Gemeentelijk managementteam (GMT)	Het GMT adviseert het college over de te stellen kaders en is verantwoordelijk voor de nadere uitwerking van het informatiebeveiligingsbeleid binnen die kaders en de sturing daarop.
Informatiebeveiligingsdienst (IBD)	De IBD is onderdeel van de Vereniging van Nederlandse Gemeenten en ondersteunt gemeenten op het gebied van informatiebeveiliging en privacy.
Privacy by Default	Privacy by default kan gezien worden als een onderdeel van privacy by design. Privacy by default vereist dat de standaardinstellingen altijd zo privacy-vriendelijk mogelijk zijn. Er moet voor gezorgd worden dat persoonsgegevens nooit standaard openbaar zichtbaar zijn.
Privacy by Design	De letterlijke vertaling van privacy by design is: gegevensbescherming door ontwerp. Het idee is om al in een vroeg stadium zowel technisch als organisatorisch een zorgvuldige omgang met persoonsgegevens af te dwingen. Het houdt in dat er al bij de ontwikkeling van producten en diensten aandacht moet zijn voor privacy.
SUWI	Wet Structuur Uitvoeringsorganisatie Werk en Inkomen
SUWInet	Via Suwinet Services kunnen overheidsorganisaties gegevens van burgers en bedrijven digitaal bij elkaar opvragen en naar elkaar sturen. Door gegevens binnen de overheid te delen kunnen burgers sneller en beter worden geholpen en hoeven zij geen gegevens te verstrekken die de overheid al heeft. Suwinet Services zijn primair bedoeld voor UWV, SVB en de gemeentelijke sociale diensten, maar inmiddels maken ook andere overheidsorganisaties gebruik van Suwinet Services.
Verwerker	Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder aan zijn rechtstreeks gezag te zijn onderworpen.
Verwerkersovereenkomst	In een Verwerkersovereenkomst leggen een Verantwoordelijke en een Verwerker onder andere samenwerkingsafspraken over de verwerking van gegevens vast.
Verwerkingsregister	In de AVG staan een aantal verplichte maatregelen genoemd waarmee aan de verantwoordingsplicht kan worden voldaan. Een van die verplichtingen is het 'register van verwerkingsactiviteiten'. Of het register moet worden opgesteld, hangt af van de omvang van de organisatie en het type gegevens dat wordt verwerkt.

.

[1] Ook wel ''Data Protection Officer''.

1. Inleiding

1.1 Achtergrond

Privacy en de bescherming van persoonsgegevens is een belangrijk thema binnen gemeenten. Zo wordt er 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.

Gemeenten zijn verantwoordelijk voor de uitvoering van taken in het sociaal domein, zoals taken op het gebied van de Jeugdwet, de Wet maatschappelijke ondersteuning (Wmo 2015), de Participatiewet, de Wet gemeentelijke schuldhulpverlening etc. Hierdoor wordt in het sociaal domein meer gewerkt met gegevens dan in andere delen van de gemeentelijke organisatie. Daarbij gaat het veelvuldig om verwerking van gevoelige gegevens zoals medische, financiële en/of strafrechtelijke gegevens. De taken in het sociaal domein worden op verschillende manieren uitgevoerd en gemeenten werken daarbij samen met verschillende organisaties. Het werken met (gevoelige) persoonsgegevens en het delen ervan in verschillende samenwerkingsverbanden brengt (extra) nieuwe privacyrisico's met zich mee. Het is van belang dat gemeenten (en andere betrokken partijen) zich hiervan bewust zijn, zo ook de gemeente Rijswijk.

In alle gemeenten bestaat er een bepaalde mate van spanning tussen het verlenen van kwalitatief goede en snelle dienstverlening enerzijds en het beschermen van de privacy van burgers anderzijds.[2] De invoering van de AVG maakt dat gegevensdeling alleen kan op basis van zes grondslagen.[3] De strengere wet- en regelgeving rondom privacy kan ervoor zorgen dat medewerkers binnen het sociaal domein uit angst de regels te overtreden belangrijke informatie niet delen. Dit kan voor inwoners frustrerend zijn, omdat zij door gebrekkige gegevensdeling binnen de gemeente hetzelfde verhaal aan meerdere medewerkers moeten vertellen.

Een ander (vergelijkbaar) spanningsveld zit tussen integraal werken en het beschermen van privacy. Door de decentralisaties zijn er 'schotten' geplaatst tussen de drie domeinen: jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen. Om integraal te werken kan gegevensdeling tussen deze domeinen noodzakelijk zijn. Denk bijvoorbeeld aan een burger met schuldenproblematiek. Het is goed mogelijk dat deze problematiek bekend is bij de consulenten van het werkbedrijf, maar niet bij medewerkers van een sociaal wijkteam vanwege de wet- en regelgeving rondom privacy. Dit zorgt ervoor dat het integraal werken van de gemeente wordt bemoeilijkt. Het spanningsveld kan ook andersom werken: gemeenten doen regelmatig een brede uitvraag om multiproblematiek van burgers in kaart te brengen. Hierbij stelt de gemeente vragen over meerdere leefgebieden. De burger kan dit ervaren als een inbreuk op zijn of haar privacy.

[2] NVRR, Handreiking rekenkameronderzoek naar privacy in het Sociaal Domein, november 2020.
[3] De grondslagen op basis waarvan persoonsgegevens mogen worden verwerkt voor een organisatie zijn: 1) toestemming van de persoon over wie het gaat; 2) als het wettelijk noodzakelijk is bij het uitvoeren van een overeenkomst; 3) bij wettelijke plichten; 4) als het noodzakelijk is om een taak van algemeen belang of openbaar gezag uit te voeren; 5) als het noodzakelijk is om een gerechtvaardigd belang te behartigen; 6) als het noodzakelijk is om vitale belangen te beschermen.

De rekenkamercommissie wil graag inzicht verkrijgen in hoe de gemeente invulling geeft aan de borging van privacy en de bescherming van persoonsgegevens in het sociaal domein van de gemeente Rijswijk.

1.2 Doelstelling, onderzoeksvragen en normenkader

Het doel van dit onderzoek is om inzicht te verkrijgen in de huidige staat van de bescherming van persoonsgegevens bij de gemeente Rijswijk en de gevolgen hiervan, alsmede het formuleren van concrete verbeteracties. De centrale onderzoeksvraag van dit onderzoek luidt dan ook:

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

Deelvragen en normenkader

Om de centrale onderzoeksvraag te kunnen beantwoorden, hebben we enkele deelvragen geformuleerd. Per vraag hebben we ook een of meerdere normen opgenomen. De bevindingen van het onderzoek zijn getoetst aan het normenkader.

Onderzoeksvragen	Normen
1. Beleid	
1.1 Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de juridische borging van de privacy van de inwoners? 1.2 In hoeverre voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormkader Baseline Informatiebeveiliging Gemeenten (BIO) en aan de Algemene Verordening Gegevensbescherming (AVG)?	▪ De gemeente heeft (SMART-opgestelde) beleidskaders, regels en richtlijnen voor het juridisch borgen van de privacy van inwoners; ▪ Het beleid en de uitwerking in processen van de gemeente voldoet aan de bepalingen van de BIO; ▪ Het beleid en de uitwerking van processen van de gemeente voldoet aan de bepalingen van de AVG.
2. Organisatie en uitvoering	
2.1 Hoe is het privacybeleid uitgewerkt en geborgd in processen op de werkvloer en is het beleid duidelijk voor de verantwoordelijke uitvoerders (consulenten)? 2.2 Zijn er casussen waarin sprake is van schending van de privacy van inwoners en hoe is daarmee omgegaan? 2.3 Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van de inwoners? 2.4 In hoeverre zijn de functionaris gegevensbescherming (FG), Chief Information Security Officer (CISO), adviseur informatieveiligheid en de privacy adviseur(s) op	▪ Het privacybeleid van de gemeente is uitgewerkt en geborgd in processen op de werkvloer; ▪ Het privacybeleid is duidelijk en werkbaar voor de verantwoordelijke uitvoerders (consulenten); ▪ In het geval van privacyschending van inwoners is er een duidelijk ‘stappenplan’ en zijn er verantwoordelijken om de privacyschending op te lossen; ▪ De gemeente betrekt medewerkers bij het borgen van privacybeleid door middel van trainingen; ▪ De FG, CISO, adviseur informatieveiligheid en privacy adviseur(s) worden in staat gesteld om

de hoogte van de geldende kaders, regels en verantwoordelijkheden van de BIO en de AVG?	(bijvoorbeeld via trainingen) op de hoogte te blijven van (technologische) ontwikkelingen op het gebied van data en actuele kennis omtrent de BIO/AVG.
3. Risico's en borging privacy	
3.1 Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van de inwoners is geborgd binnen de gemeente? 3.2 Hoe ziet de gemeente erop toe dat de borging van privacy van een voldoende niveau is en blijft, en wordt er geanticipeerd op toekomstige opgaven en juridische ontwikkelingen?	▪ De gemeente heeft inzichtelijk welke (mogelijke) risico's bestaan in de huidige borging van en werkwijze voor privacy; ▪ De gemeente anticipeert op en handelt naar alles wat een (potentiële) bedreiging vormt voor het niveau van de borging van de privacy van inwoners; ▪ Door middel van (beleids)stukken omschrijft de gemeente een duidelijke visie als het gaat om toekomstige opgaven en juridische ontwikkelingen voor privacy, en heeft de bijbehorende verantwoordelijkheid belegd in de organisatie zodat de visie wordt vertaald naar de praktijk.
4. Communicatie met inwoners	
4.1 Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?	▪ De gemeente communiceert op een duidelijke, transparante en systematische wijze naar haar inwoners toe over privacy en hoe zij daarmee omgaat; ▪ De gemeente voldoet aan de informatieplicht zoals vastgelegd in de AVG.
5. Sturing en controle	
5.1 Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid en informatieveiligheid in het sociaal domein betrokken geweest? 5.2 Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?	▪ De raad is betrokken (geweest) bij de ontwikkeling van het privacybeleid en informatieveiligheid in het sociaal domein, bijvoorbeeld door middel van raadsinformatiebrieven of een privacy expert die aansloot bij een raadsvergadering; ▪ Het college brengt de raad in positie om toezicht te houden en te controleren, bijvoorbeeld door regelmatig inzicht te geven in privacyschendingen en geïmplementeerde oplossingen; ▪ De raad geeft invulling aan zijn toezichthoudende en controlerende taak (en stelt bijvoorbeeld vragen over de realisatie).

Afbakening

Het onderzoek richt zich op:

- Het privacybeleid en de informatieveiligheid in het Sociaal Domein van de gemeente Rijswijk. Hierbij wordt gefocust op de periode sinds het ingaan van de AVG, sinds 25 mei 2018.

Het onderzoek richt zich niet op:

- Het privacybeleid en de informatieveiligheid in andere domeinen van de gemeente Rijswijk.

1.3 Onderzoeksmethoden

Dit onderzoek vond plaats in de periode maart t/m juni 2021. In het kader van het onderzoek hebben deskresearch en interviews plaatsgevonden.

Deskresearch

Allereerst heeft er in het kader van dit onderzoek deskresearch plaatsgevonden. Zo zijn er (beleids)documenten van de gemeente Rijswijk, landelijke rapportages en richtlijnen en ook andere rekenkameronderzoeken bestudeerd.

Interviews

In totaal hebben er zeven interviews plaatsgevonden (zie bijlage 1). In maart 2021 vond er een startgesprek plaats met de manager bedrijfsvoering sociaal domein, met wie ook in april 2021 nog een vervolggesprek heeft plaatsgevonden. Binnen de ambtelijke organisatie is er verder gesproken met de CISO, de FG, de privacy officer en de senior kwaliteitsmedewerker/AVG/BIO. Met deze sleutelpersonen werd gesproken over het beleid en de uitvoering daarvan, de mogelijke risico's voor gegevensbescherming in Rijswijk, het informatiebewustzijn binnen de gemeente, de communicatie met burgers en de informatievoorziening aan de raad. Om inzicht te krijgen in de dagelijkse praktijk van het sociaal domein werd er ook gesproken met twee consulenten uit het sociaal domein. Ten slotte is er gesproken met de portefeuillehouder.

Met de inzichten die zijn verkregen met behulp van de deskresearch en de interviews wordt het gevoerde beleid en de praktijk van de borging van privacy in Rijswijk beoordeeld aan de hand van het normenkader, en een antwoord geformuleerd op de centrale onderzoeksvraag.

1.4 Leeswijzer

In hoofdstuk 2 wordt het beleid ten aanzien van privacy en informatieveiligheid beschreven. In hoofdstuk 3 wordt ingegaan op de wijze waarop privacy en informatieveiligheid een plek hebben in de processen en in hoofdstuk 4 de wijze waarop dit is belegd in de organisatie van Rijswijk en meer specifiek het sociaal domein. In hoofdstuk 5 wordt verkend hoe de gemeente communiceert met haar inwoners over (de borging van) privacy en de (mogelijke) gevolgen van privacyregels en informatiebeveiliging. In hoofdstuk 6 wordt ingegaan op de risico's voor de huidige borging van privacy en toekomstige opgaven en ontwikkelingen. Vervolgens wordt in hoofdstuk 7 ingegaan op de informatievoorziening aan omtrent - en de rol van de raad bij - het thema privacy en informatieveiligheid. In hoofdstuk 8, tot slot, worden de resultaten van dit onderzoek geanalyseerd en worden conclusies getrokken en aanbevelingen geformuleerd voor verdere verbetering van privacy en informatiebeveiliging in het sociaal domein van de gemeente Rijswijk.

2. Beleid

Van belang is dat het gemeentelijk beleid voldoet aan de wettelijke kaders en de gemeente handelt naar haar wettelijke plichten op het gebied van privacy en informatiebeveiliging. Voorbeelden van plichten die de gemeente heeft, zijn het hebben van privacybeleid, het bijhouden van een verwerkingsregister, het uitvoeren van Data Protection Impact Assessments (DPIA's) en het opstellen van verwerkingsovereenkomsten. In dit hoofdstuk wordt een antwoord geformuleerd op de volgende onderzoeksvragen:

- Welke beleidskaders, regels en richtlijnen hanteert de gemeente voor de juridische borging van de privacy van de inwoners?
- In hoeverre voldoet het beleid en de uitwerking in processen binnen de gemeente aan de bepalingen van het basisnormenkader Baseline Informatiebeveiliging Gemeenten (BIO) en aan de Algemene Verordening Gegevensbescherming (AVG)?

2.1 Kaderstelling privacy en informatieveiligheid

De gemeente hanteert de volgende beleidskaders: het privacybeleid en privacyreglement, het informatiebeveiligingsbeleid, het informatiebeleidsplan 2020-2022 en het informatiebeveiligingsplan 2020. Daarnaast hanteert de gemeente de regels en richtlijnen zoals de Borgingscriteria AVG van de Informatiebeveiligingsdienst (IBD), de handreiking AVG van de IBD en VNG en de handreiking introductie aanpak BIO van de IBD.

2.1.1 Privacybeleid

Het domeinoverstijgend privacybeleid van Rijswijk trad in mei 2018 in werking en wordt eens per twee jaar geëvalueerd en waar nodig herzien. Middels dit beleid geeft de gemeente richting aan privacy en wil de gemeente laten zien privacy te waarborgen, beschermen en handhaven. De gemeente zorgt ervoor dat privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole. Bij het werken met persoonsgegevens, werkt de gemeente aan de hand van negen uitgangspunten: rechtmatigheid, behoorlijkheid en transparantie, grondslag en doelbinding, dataminimalisatie, bewaartermijn, integriteit en vertrouwelijkheid, delen met derden, subsidiariteit, proportionaliteit en de rechten van betrokkenen.[4] Daarmee sluit het beleid aan op de beginselen uit de AVG: behoorlijkheid, transparantie, doelbinding, dataminimalisatie, opslagbeperking, juistheid, integriteit en vertrouwelijkheid. De Autoriteit Persoonsgegevens (AP) deed eerder zes aanbevelingen aan organisaties om hun privacybeleid goed in te richten. Een van de aanbevelingen is: ''Wees concreet; een gegevensbeschermingsbeleid is een concrete vertaalslag van de AVG-normen naar de gegevensverwerkingen van een organisatie. Normen uit de AVG herhalen is niet voldoende''.[5] De gemeente Rijswijk heeft gebruik gemaakt van het VNG Model Privacybeleid en -Reglement voor gemeenten. Het privacybeleidskader en de daarin geformuleerde uitgangspunten van de gemeente Rijswijk heeft een algemeen karakter. Het beleid zoomt niet in op de spelregels die kunnen gelden voor specifieke beleidsterreinen. Daarnaast ontbreekt het aan SMART-opgestelde beleidskaders, regels en

[4] Voorbeelden van rechten die betrokkenen (degenen van wie persoonsgegevens worden verwerkt) kunnen uitoefenen zijn: het recht op informatie, het recht op inzage, het recht op rectificatie, het recht op gegevenswissing (vergetelheid), het recht op beperking van de verwerking, het recht op overdraagbaarheid (dataportabiliteit), het recht van bezwaar, het recht niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profilering.

[5] Autoriteit Persoonsgegevens, Zes aanbevelingen voor een privacybeleid, 17 april 2019 (https://autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid).

richtlijnen voor het juridisch borgen van privacy van inwoners. De VNG verwijst naar het privacybeleid van de gemeente Leidschendam-Voorburg als voorbeeld.[6] Een ander voorbeeld is het privacybeleid van de gemeente Nunspeet.[7]

Bevindingen
- Het privacybeleid van de gemeente is in lijn met de AVG.
- De gemeente heeft de normen uit de AVG eenvoudigweg herhaald en niet nader geconcretiseerd. Dit is volgens de AP niet voldoende.

2.1.2 Informatiebeveiligingsbeleid

Informatieveiligheid en privacy is onderdeel van het door de raad vastgestelde informatiebeleidsplan 2020-2022 (IBP). Doel van dit IBP is het formuleren van een visie en het inzichtelijk maken van kaders en kwaliteitseisen voor de informatievoorziening bij de gemeente Rijswijk.[8]

Informatiebeveiligingsbeleid

In het informatiebeveiligingsbeleid stelt het college de kaders en geeft het richtlijnen aan de uitvoering over de inrichting van de informatiebeveiliging: welke normen worden gehanteerd en hoe zijn de verantwoordelijkheden verdeeld. Het belangrijkste uitgangspunt van het informatieveiligheidsbeleid is dat de gemeente Rijswijk zich conformeert aan de Baseline Informatiebeveiliging Overheid.[9] Voor de ondersteuning van bestuurders bij de uitvoering van goed risicomanagement zijn door de VNG in aanvulling op de BIO de tien bestuurlijke principes voor informatiebeveiliging opgesteld.[10] Dit informatiebeveiligingsbeleid wordt minimaal één keer per drie jaar beoordeeld en zonodig bijgesteld.

Informatiebeveiligingsplan

Binnen de 3-jaarlijkse kwaliteitscyclus van het informatiebeveiligingsbeleid wordt een actieplan (informatie*beveiligings*plan) opgesteld dat gebaseerd is op de zelfevaluatie in de Eenduidige Normatiek Single Information Audit (ENSIA). Het plan wordt geschreven onder verantwoordelijkheid van de CISO. Het plan wordt jaarlijks beoordeeld en waar nodig herzien. Het geeft een overzicht van de te realiseren verbeterpunten waarbij een voorstel voor de aanpak ervan en de opgave van de (coördinerende) actiehouder is benoemd.[11]

Bevindingen
- Er is sprake van kaderstelling in het informatiebeveiligingsbeleid. De gemeente heeft het beleid - dat opgesteld is aan de hand van de BIO - uitgewerkt in het informatiebeveiligingsplan.

[6] https://www.informatiebeveiligingsdienst.nl/wp-content/uploads/2019/03/Handreiking-en-voorbeeld-privacybeleid-Leidschendam-Voorburg.pdf
[7] Privacybeleidskader Gemeente Nunspeet 2020-2024, https://zoek.officielebekendmakingen.nl/gmb-2021-101255.html
[8] Gemeente Rijswijk, Informatiebeleidsplan 2020-2022.
[9] Gemeente Rijswijk, Informatiebeveiligingsbeleid 2020.
[10] Zie: https://vng.nl/files/vng/de-10-bestuurlijke-principes-voor_20190109.pdf
[11] Gemeente Rijswijk, Informatiebeveiligingsplan 2020.

3. Processen

De gemeente is verantwoordelijk voor het opstellen, uitvoeren en handhaven van het beleid. Van belang om te weten is in hoeverre het privacybeleid is uitgewerkt en geborgd in processen. Hiervoor gelden onder andere de wettelijke kaders van de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet AVG.[12] Daarnaast is met ingang van 1 januari 2020 de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO is een doorontwikkeling van de Baseline Informatieveiligheid voor Gemeenten (BIG). Hiermee ontstaat één gezamenlijk normenkader voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek. De volgende onderzoeksvraag komt aan bod in dit hoofdstuk:

- Hoe is het privacybeleid uitgewerkt en geborgd in processen op de werkvloer?

3.1 Uitwerking en borging van privacy(beleid) in processen

Privacybescherming is een continu proces. De werkprocessen die persoonsgegevens bevatten moeten getoetst en ingericht worden volgens de beginselen uit de AVG en de uitgangspunten uit het privacybeleid van de gemeente Rijswijk. Daarvoor heeft de Functionaris Gegevensbescherming (FG) allereerst het 10-stappenplan van de AP geïmplementeerd binnen de gemeente.[13] Zo zijn er processen en procedures ontwikkeld, is er een datalekkenregister, een verwerkingsregister, en zijn er mogelijkheden voor inwoners om hun rechten uit te oefenen. Daarnaast zijn er maatregelen ingevoerd zoals bewustwordingsmaatregelen, DPIA's, Privacy by Design & Privacy by Default, en is er gekeken naar de wijze waarop de gemeente omgaat met toestemming voor gegevensverwerking van betrokkenen. Al de processen en de maatregelen in het sociaal domein - en in het algemeen - zijn van belang om privacy goed te borgen. Dat houdt bijvoorbeeld in dat de systemen ''privacy by design'' zijn en dat processen zodanig zijn ingericht dat niet iedere medewerker overal bij kan. Voor nu richten de FG en zijn team zich op de kwaliteit van de processen en controleren zij of de autorisatieschema's op orde zijn. De focus ligt daarmee op risicogestuurde werkzaamheden.

Procedure melden datalekken en datalekkenregister

De gemeente Rijswijk heeft procedures en werkinstructies voor het omgaan met en het melden van datalekken. Deze staan op Intranet (Edison). Tevens wordt er een register met datalekken bijgehouden.

Verwerkingsregister

De senior adviseur Kwaliteit coördineert de borging van de AVG in het sociaal domein. De gemeente houdt een register van verwerkingsactiviteiten bij. Daarin zijn de verwerkingen van persoonsgegevens waar de gemeente Rijswijk verwerkingsverantwoordelijk of medeverantwoordelijk voor is in opgenomen. De geplande toets of alle verwerkingen binnen de gemeente een doel en een grondslag hebben en of deze aan de beginselen van proportionaliteit, subsidiariteit en dataminimalisatie voldoen, heeft in 2020 niet plaats kunnen vinden omdat de organisatie de werkprocessen, waarin

[12] Uit de jaarrapportage van de FG volgt dat naast het algemeen wettelijk kader van de AVG er in sectorspecifieke wetten aanvullende regels opgenomen zijn over gegevensuitwisseling en het waarborgen van privacy. Voorbeelden van deze wetten zijn de Wmo 2015, de Jeugdwet, de Participatiewet, de BRP etc. De kennis van de materiewetten is bij de teams aanwezig en de uitvoering hiervan is een operationele taak van de teams. In de processen van de betreffende domeinen is hiermee nog onvoldoende rekening gehouden.

[13] Het 10-stappenplan ter voorbereiding op de AVG is - nu de privacywet in werking is getreden - vervangen door de checklist 'houd grip op persoonsgegevens'.

persoonsgegevens worden verwerkt, niet overal beschreven had.[14] De privacyjurist pakt dat in juni van 2021 op. Op termijn wil de gemeente deze toets in de P&C cyclus borgen, zodat altijd wordt gecontroleerd hoe verwerkingsactiviteiten in het verwerkingsregister staan, of er sprake is van een verwerking en of het register moet worden ingevuld of geactualiseerd.

DPIA's

De gemeente is in specifieke gevallen verplicht om een Data Protection Impactanalyse (DPIA)[15] uit te voeren. Dat is bijvoorbeeld het geval wanneer er sprake is van het gebruik van een nieuwe applicatie waarin verwerkingen van gegevens voorkomen. Via deze risicoanalyse wordt de rechtmatigheid van de verwerking getoetst en wordt gecontroleerd of de gegevensverwerking een hoog privacyrisico oplevert voor de betrokkene. De gesprekspartners geven aan dat de gemeente niet alleen de nieuwe, maar ook de bestaande processen tegen het licht zou moeten houden. Dat is echter nog niet geregeld. In het sociaal domein kan er regelmatig gebruik worden gemaakt van generieke DPIA's die op regionaal of landelijk niveau zijn uitgevoerd, zoals het geval is met de vernieuwde Wet gemeentelijke schuldhulpverlening. Die DPIA's kan de gemeente spiegelen aan de eigen organisatie. Een overzicht van de reeds uitgevoerde DPIA's is opgenomen in het jaarverslag van de FG.

Autorisaties

Toegang tot informatiesystemen is in principe beperkt tot bevoegde medewerkers door middel van autorisaties. Het is van belang dat zaken vastgelegd en navolgbaar zijn. Dat heeft de gemeente niet altijd op orde. Een voorbeeld daarvan is het ontbreken van de autorisatiematrix, waardoor er niet met zekerheid kan worden gezegd dat aan alle risico's is gedacht. De proceseigenaren moeten de autorisatiematrix vaststellen middels een besluit. Dat besluit is niet altijd aantoonbaar genomen. In het sociaal domein is de autorisatiematrix en het besluit soms wel aanwezig. Dat geldt bijvoorbeeld voor Suwinet. Uit de gesprekken volgt dat de gemeente momenteel actief bezig is met het controleren van autorisaties.

Privacy by Design en Privacy by Default

Bij de inrichting van nieuwe systemen wordt nog niet altijd rekening gehouden met de beginselen van Privacy by Design (dataminimalisatie) en Privacy by Default (privacy-vriendelijke instellingen als standaard).[16]

Logging

Door middel van logging legt een organisatie gebeurtenissen in het systeem vast. Bijvoorbeeld, wie bepaalde gegevens heeft bekeken of aangepast, maar ook pogingen om ongeautoriseerd toegang te krijgen. Er is in Rijswijk geen algemeen loggingbeleid en niet alle geautomatiseerde systemen zijn voorzien van logging. Voor de realisatie daarvan is de gemeente afhankelijk van het ontwikkeltempo van de leveranciers.[17]

[14] Jaarrapportage van de FG 2020.
[15] Een DPIA is een risicoanalyse en wordt ook wel PIA of gegevensbeschermingseffectbeoordeling (GEB) genoemd.
[16] Jaarrapportage van de FG 2020.
[17] Jaarrapportage van de FG 2020.

Bevindingen:

- Met de implementatie van het 10-stappenplan van de AP staat de basis. Op hoofdlijnen zijn de processen op orde, tegelijk zijn er enkele verbeterpunten (zie hieronder).
- De gemeente voert nog geen risicoanalyses (DPIA's) uit op bestaande processen.
- Autorisaties zijn niet altijd navolgbaar.
- De gemeente houdt nog niet altijd rekening met de beginselen van Privacy by Design en Privacy by Default.
- Het loggingbeleid is nog niet helemaal op orde.

3.1.1 De AVG en processen in het sociaal domein

Het is lastig te zeggen in hoeverre specifiek de processen van het sociaal domein voldoen aan de AVG. Op basis van de interviews kan gezegd worden dat het sociaal domein wat betreft procesbeschrijving al een stuk verder is dan andere onderdelen van de organisatie. Daarbij komt dat het college per 1 januari 2021 capaciteit heeft gecreëerd in de rol van de senior Adviseur Kwaliteit voor de implementatie van de BIO en de AVG in het sociaal domein. Zij gaat kijken hoe het sociaal domein van de gemeente ervoor staat met de AVG en de BIO, wat anders kan en wat de aandachtspunten zijn. Ook zet zij processen op papier of is ze nauw betrokken (geweest) bij het beschrijven van (recente) processen. De gemeente heeft ervoor gekozen om de borging van de AVG en de BIO bij Kwaliteit te beleggen, zodat het in de PDCA-cyclus wordt geborgd. Op basis van de acties uit het jaarverslag van de FG (2020) is deze adviseur concreet gestart met het opstellen van een plan voor het realiseren van de verbeteracties die voortkomen uit de borgingscriteria AVG. De uitvoering van de verbeteracties uit het plan wordt gemonitord en periodiek gerapporteerd aan het GMT.[18] Daarmee is er ook een start gemaakt met de benodigde verdiepingsslag. Ook denkt zij mee over onderwerpen als het uitvoeren van DPIA's, het sluiten van verwerkersovereenkomsten en houdt zij het verwerkingsregister bij.

3.1.2 Zelfevaluatie

De VNG biedt een checklist om te controleren in hoeverre de gemeente voldoet aan de wettelijke kaders en handelt naar haar wettelijke plichten.[19] Het zogenaamde borgingsproduct ''Borgingscriteria AVG'' en de controls zijn verdeeld in zeven thema's. De thema's zijn: Beleid, Organisatorische inbedding, Processen, Rechten van betrokkenen, Samenwerking, Beveiliging, en Verantwoording. De risicogestuurde aanpak staat centraal. De gemeente Rijswijk heeft op basis van het borgingsproduct zelf een evaluatie uitgevoerd over het jaar 2020. Daaruit volgt in hoeverre er gemeentebreed wordt voldaan aan de borgingscriteria. De uitkomst daarvan wordt door middel van enkele diagrammen en het daarbijbehorende percentage van compliance weergegeven in bijlage 2.[20] In april 2021 publiceerde de VNG een handreiking (ter vervanging van de ''Borgingscriteria AVG'') dat het niveau van privacyborging koppelt aan zogenoemde ''privacyvolwassenheidsniveaus'': het Borgingsproduct 2.0. Aan de hand daarvan kan de gemeente per thema en afdeling een ambitieniveau vaststellen.[21] Bijlage 3 bevat een overzicht met uitleg over de privacyvolwassenheidsniveaus. Dit nieuwe borgingsproduct zal worden gebruikt bij het opstellen van het jaarverslag van de FG in 2021. Het

[18] Gemeente Rijswijk, Informatiebeleidsplan 2020.
[19] Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie: https://www.vngrealisatie.nl/sites/default/files/2018-11/dec2018%20criteria%20borging%20AVG%20VNG%20Realisatie.pdf
[20] Zo voldoet het beleid bijvoorbeeld aan 14 van de 15 borgingscriteria. Wat betreft de werkprocessen wordt er geheel voldaan aan 18 criteria en gedeeltelijk voldaan aan 8 criteria van de in totaal 33 borgingscriteria.
[21] Informatiebeveiligingsdienst en VNG, Handreiking AVG Borgingsproduct 2.0, 8 maart 2021.

borgingsproduct ''Borgingscriteria AVG'' dat werd gebruikt voor het jaar 2020 gaf nog geen mogelijkheid om de volwassenheidsniveaus te berekenen.

Het resultaat van de zelfevaluatie wordt opgenomen in de jaarrapportage van de FG. In het jaarverslag geeft de FG inzicht in de mate waarin de gemeente Rijswijk aan de AVG voldoet en de belangrijkste resultaten van dat jaar. Ook wordt vooruitgekeken naar de werkzaamheden en uitdagingen voor het volgend jaar.

Bevindingen
- Het sociaal domein loopt voorop in de organisatie wat betreft procesbeschrijving. Privacy is in de PDCA-cyclus geborgd en is er een start gemaakt met de verdiepingsslag in het sociaal domein.
- De gemeente voert een zelfevaluatie naar privacyborging uit. Met de doorontwikkeling van deze evaluatie kan de gemeente naar verwachting in 2022 het eigen privacyvolwassenheidsniveau bepalen.
- Met de jaarrapportage van de FG wordt de AVG vertaald naar een kwaliteitscyclus voor gegevensbescherming en privacy voor gemeentelijke processen.

3.2 Implementatie van de BIO

Vanaf 1 januari 2020 is de BIO van kracht. De BIO beschrijft het voor de gemeente vereiste informatiebeveiligingsniveau. Op basis daarvan is in 2020 de ENSIA-verantwoording gedaan. Op basis van de ENSIA-verantwoording schat de CISO in dat de beveiligingsmaatregelen over het algemeen op een goed niveau zitten. Er moet echter ook nog veel gebeuren. Daarom is er op basis van de uitkomsten van de ENSIA een actieplan geschreven voor de implementatie van de BIO. Een onderdeel van dat plan is dan ook dat er binnen alle domeinen een traject loopt waarin er bewustzijn wordt gecreëerd over de processen die binnen het domein aanwezig zijn. De bedoeling is dat deze eerste stap aan het eind van 2021 klaar is.

De senior adviseur Kwaliteit is betrokken bij de implementatie van de BIO in het sociaal domein. Daarvoor heeft zij onlangs een plan van aanpak opgesteld en besproken met het management.[22] De planning van het plan van aanpak voor specifiek het sociaal domein loopt tot maart 2024. De procesbeschrijvingen per bedrijfsproces zijn al geregeld in het sociaal domein. Het sociaal domein is dan ook al ''een stap verder'' als het gaat om de implementatie van de BIO. De senior adviseur Kwaliteit gaat kijken naar hoe de processen verder aangepast en verbeterd kunnen worden zodat ze voldoen een de vereisten van de BIO. Zo wordt er per bedrijfsproces nagelopen hoe het zit met autorisaties, of dat goed beschreven is en of er continuïteitsplannen bestaan voor ieder bedrijfsproces.

Bevindingen
- Voor de implementatie van de BIO in het sociaal domein is in april 2021 een plan van aanpak gemaakt. De uitvoering daarvan loopt tot 2024. Het is nog te vroeg om daar een oordeel over te kunnen vormen.

[22] Gemeente Rijswijk, Plan van aanpak invoering BIO sociaal domein, 12 april 2021.

4. Organisatie en uitvoering

Essentieel voor het omgaan met privacyvraagstukken is de inrichting van de organisatie. Dit rekenkameronderzoek beoogt de raad inzicht te bieden in de wijze waarop de verantwoordelijkheden zijn belegd binnen de organisatie en het bestuur en in hoeverre deze keuzes logisch zijn. De volgende onderzoeksvragen zullen beantwoording vinden in dit hoofdstuk:

- Is het beleid duidelijk voor de verantwoordelijke uitvoerders (consulenten)?
- Zijn er casussen waarin sprake is van schending van de privacy van inwoners en hoe is daarmee omgegaan?
- Hoe worden medewerkers betrokken bij en getraind in het borgen van de privacy van de inwoners?
- In hoeverre zijn de functionaris gegevensbescherming (FG), Chief Information Security Officer (CISO), adviseur informatieveiligheid en de privacy adviseur(s) op de hoogte van de geldende kaders, regels en verantwoordelijkheden van de BIO en de AVG?

4.1 Organisatorische inbedding

De Functionaris Gegevensbescherming is het verlengstuk van de AP en is ondergebracht in de functie van concerncontroller. Het team concerncontrol bestaat voor wat betreft privacy en informatiebeveiliging verder uit de adviseur informatieveiligheid (CISO) en de adviseur Privacy (privacy officer). De CISO focust op de implementatie van de BIO en de FG en privacy officer focussen op de implementatie van de AVG.

De FG en CISO hebben vanuit concerncontrol al een onafhankelijke positie. Bovendien rapporteren beiden rechtstreeks aan de gemeentesecretaris. De gemeentesecretaris is betrokken en wil apart geïnformeerd worden over de status van privacy en informatiebeveiliging. Ook is de gemeentesecretaris bijgepraat over bijvoorbeeld het lek bij het Hof van Twente waarmee hij dan terugkwam bij de FG en CISO en aangaf wat prioriteit had.

De privacy officer adviseert de teams. De functie van privacy officer behelst bijna alle facetten van privacybescherming: van het geven van advies over toepassing van de AVG tot het doen van onderzoek voor het jaarverslag van de FG. De privacy officer houdt de datalekken bij in het intern register en monitort de tijdige afhandeling hiervan. De CISO en de privacy officer ondersteunen de organisatie onder meer bij de uitvoering van de DPIA's. Daarnaast worden zij goed bevraagd door de organisatie over het delen van gegevens en het sluiten van verwerkersovereenkomsten; weliswaar soms iets te laat in het proces.

Er is een privacy jurist binnen het team Juridische Zaken gepositioneerd die beschikbaar is voor juridische vragen. De FG, de CISO, de privacy officer en privacy jurist komen periodiek bij elkaar om ontwikkelingen te bespreken. Samen adviseren zij de organisatie bij privacyvraagstukken en de verdere implementatie van de AVG. Zij stellen beleid op, ontwerpen processen en richtlijnen, houden registers bij en voeren audits uit. Er is sprake van een nauwe samenwerking. De privacyfunctionarissen zijn goed gepositioneerd in de organisatie, goed vindbaar en op de hoogte van de geldende kaders en regels. Uit de gesprekken blijkt dat met name de privacy officer een bekend gezicht is voor medewerkers in de organisatie. Met de komst van de privacy jurist sinds maart 2021 is de werkdruk voor de privacy officer aanzienlijk verminderd. De privacy jurist en de privacy officer zijn bijna fulltime bezig met het sociaal

domein. Dat is niet gek gezien het feit dat in het sociaal domein veelvuldig met (gevoelige) persoonsgegevens wordt gewerkt, zoals medische, financiële of strafrechtelijke gegevens. Andere organisatieonderdelen - waarin minder persoonsgegevens verwerkt worden - vragen minder aandacht. Met de komst van de senior adviseur Kwaliteit en de contractmanagers, merken ze daarin een zekere kentering. De privacy officer werkt nauw samen met de senior adviseur Kwaliteit Sociaal Domein die per 1 januari 2021 is aangesteld voor het borgen van de BIO en de AVG in het sociaal domein. Zij is het eerste aanspreekpunt binnen het sociaal domein. Met haar reeds ruime kennis van (het functioneren van) het sociaal domein is ze daar een bekend gezicht. Zij is verantwoordelijk voor het opstellen van domeinoverstijgende procedures, protocollen en werkinstructies in het sociaal domein.

Door middel van het jaarverslag legt de FG verantwoording af aan het Gemeentelijk managementteam (GMT). Het GMT stelt het jaarverslag vast dat vervolgens ter instemming aan het college van B&W wordt voorgelegd.[23] Het gemeentelijk managementteam (GMT) adviseert het college over de te stellen kaders en is verantwoordelijk voor de nadere uitwerking van het informatiebeveiligingsbeleid binnen die kaders en de sturing daarop. Ook zorgt het GMT ervoor dat voor alle processen en (ketens van) informatiesystemen een domeinmanager als eigenaar is aangewezen.[24] De primaire toepassing van de privacyregels ligt dan ook bij de proceseigenaren, oftewel het lijnmanagement.[25] De domeinmanagers zijn verantwoordelijk voor het naleven van de AVG binnen het eigen domein. Daarom is van belang is dat zij het belang inzien van privacy zodat zij erop toezien dat de privacyregels worden nageleefd en toegepast in de praktijk. Alvorens zij persoonsgegevens verstrekken aan een externe partij, horen ze advies bij het privacyteam in te winnen. Ook horen ze de FG te betrekken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Dit gebeurde in 2020 niet altijd en niet tijdig.[26]

Kennis en kunde van de privacyfunctionarissen

De FG, CISO en privacy adviseurs krijgen alle gelegenheid om hun kennis actueel te houden. Via nieuwsbrieven en meldingen van de Informatiebeveiligingsdienst (IBD) worden zij actief geïnformeerd. Ook organiseert de IBD bijeenkomsten waarin dieper wordt ingegaan op bepaalde onderwerpen (tegenwoordig in de vorm van webinars). In de regio is er een netwerkorganisatie opgericht met het doel om kennis te delen (Hacklanden). Daarnaast kunnen zij naar eigen inzicht aanvullende trainingen en cursussen volgen. Alle aanvragen aan het management voor het volgen van opleidingen en trainingen en het bijwonen van kennisdagen, congressen etc. worden tot nu toe gehonoreerd. Zo gaat de privacy officer samen met de senior adviseur Kwaliteit een Leergang ‘organiseren privacy en gegevensdeling’ volgen van de VNG. De leergang gaat specifiek in op de procesinrichting rondom casuïstiek op het snijvlak van zorg en veiligheid, met de bedoeling om privacy en gegevensdeling dusdanig te organiseren dat consulenten optimaal ondersteund worden bij omgaan met privacy dilemma's.

[23] Zie hoofdstuk 5: Het college van B&W is politiek verantwoordelijk voor het bewerkstelligen van een passend niveau van informatiebeveiliging en gegevensbescherming. Formeel gezien houdt de raad horizontaal toezicht op privacy informatiebeveiliging.
[24] Gemeente Rijswijk, Matrix rollen en bevoegdheden.
[25] Gemeente Rijswijk, Jaarrapportage van de FG 2020.
[26] Jaarrapportage van de FG 2020.

4.2 Datalekken

Wanneer er sprake is van een datalek is de proceseigenaar - dat is de manager van het team - verantwoordelijk voor het dichten van het lek. Dat betekent dat de manager het datalek binnen 24 uur moet melden bij de privacy officer en de FG. Uit de interviews komt naar voren dat medewerkers bekend zijn met de procedure. Zij weten wat ze moeten doen en bij wie ze moeten zijn als er sprake is van een datalek. Zo geven ze aan dat een datalek zo snel als mogelijk (en binnen 24 uur) moet worden gemeld bij de leidinggevende, die het vervolgens oppakt. De geraadpleegde medewerkers hebben het idee dat die procedure ook goed tussen de oren van de managers zit.

Herkennen van een datalek

Tijdens de interviews zijn er verschillende geluiden te horen wat betreft bewustzijn over (het effect van) datalekken. Zo is enerzijds duidelijk dat bij medewerkers voldoende bewustzijn heerst over wat een datalek is en over de problemen die een datalek kan veroorzaken; met name wanneer het om gegevens gaat die naar externen zijn gelekt. Anderzijds zijn sommige medewerkers niet goed op de hoogte van wat een datalek is of herkennen ze het niet. Mede daarom is bewustwording een blijvend verbeterpunt.

Melden datalekken door externen

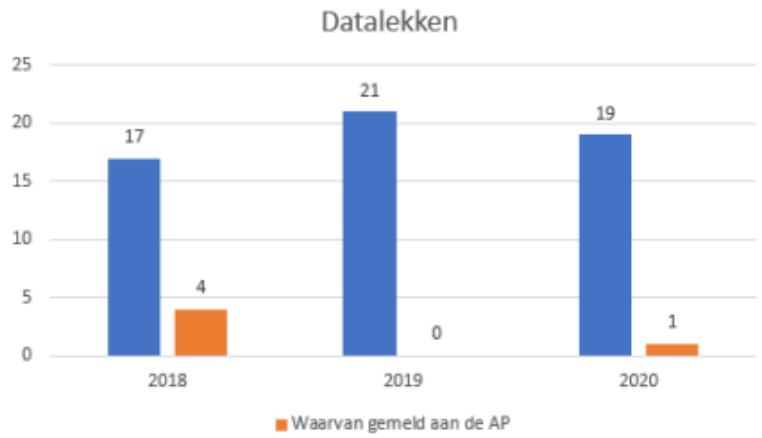
De gemeente ontdekt een datalek meestal door een melding van een burger. De gemeente heeft een aantal kanalen, waaronder de website, waarop burgers een datalek kunnen melden. Nog niet duidelijk is hoe de procedure voor het melden van datalekken werkt buiten kantoortijden.

Niet alle datalekken worden ontdekt of kunnen worden gedicht. De gemeente is daarin namelijk deels afhankelijk van de burger in de zin van dat het niet zeker is of alle inwoners een datalek herkennen of - als ze het herkennen - het melden. Daarbij komt dat wanneer de burger het lek wel meldt, de gemeente alsnog niet zeker weet of de burger de (verkeerde) informatie ook daadwerkelijk vernietigt of verwijdert. Mede daarom worden datalekken ook gezien als ''moeilijk beheersbaar''. Op basis van hoe groot het risico is, wordt de afweging gemaakt of de betrokkenen (degene van wie de informatie gelekt is) geïnformeerd moeten worden. De privacy officer informeert de FG daarover die vervolgens het besluit neemt.

Hoeveelheid en omgaan met datalekken

Uit het register datalekken blijkt dat er in 2018 zo'n 17 datalekken waren. In 2019 waren er dat 21 en in 2020 ging het om 19 datalekken (zie figuur 1). Veruit de meeste van de datalekken in 2020 hadden betrekking op het verzenden van post of e-mails aan een verkeerde persoon.[27] In het sociaal domein is dat een hoger risico, omdat er meer wordt gecommuniceerd met burgers dan in andere domeinen. Een andere oorzaak van een datalek was bijvoorbeeld een foutieve autorisatie. De organisatie duidt ongeveer de helft van de datalekken als 'menselijke fout'. Daarmee kwalificeert de gemeente de fout als een individuele fout en niet als systeemfout. Hoewel de gemeente in sommige gevallen alsnog preventieve maatregelen neemt, kan de kwalificatie als individuele fout het leren op organisatieniveau bemoeilijken.

[27] Bij het verzenden van brieven wordt geadviseerd om het vier ogen principe toe te passen. In coronatijd was dat echter niet mogelijk.



Figuur 1: Aantal datalekken in 2018, 2019 en 2020

Enkele voorbeelden van datalekken en hoe daarmee is omgegaan:

- Paspoort verzonden naar een verkeerd adres;
- Een email met toestemmingsformulier werd door een Jeugdteamlid verzonden aan de verkeerde persoon;
- Inwoner A heeft niet alleen eigen ondersteuningsplan maar ook ondersteuningsplan van inwoner B ontvangen via de post;

Melden aan de AP

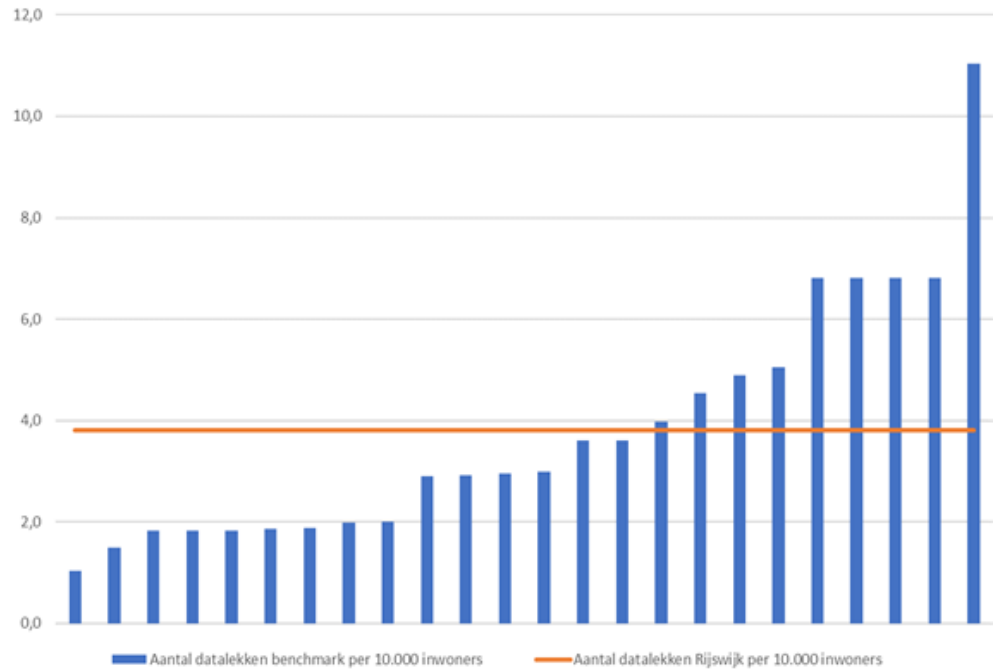
Het melden van datalekken aan de AP gebeurt relatief weinig (zie hieronder). De FG en privacy officer beslissen of het datalek wordt gemeld bij de AP. Het melden van een datalek bij de AP hangt af van de waarschijnlijkheid en de mogelijke ernst van het datalek voor de betrokken personen. Het datalek hoeft niet te worden gemeld als het niet waarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen.[28]

Vergelijking met andere gemeenten

Er is geen landelijke database van gemeentelijke datalekken. Om het aantal datalekken in Rijswijk in perspectief te plaatsen, zijn de datalekgegevens over 2019 van 24 gemeenten verzameld, hoofdzakelijk uit jaarverslagen van functionarissen gegevensbescherming.[29] Rijswijk heeft omgerekend 3,8 datalekken per 10.000 inwoners. Bij de 24 gemeenten in de benchmark is dat gemiddeld 4,1 datalekken per 10.000 inwoners. Het aantal datalekken in Rijswijk ligt daarmee dicht bij het benchmarkgemiddelde. De spreiding is echter aanzienlijk, zoals te zien is in figuur 2.

[28] https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

[29] Amersfoort, Beemster, Bergen (NH), Uitgeest, Castricum en Heiloo, Eindhoven, Gooise Meren, Gorinchem, Halderberge, Hilversum, Huizen, Leusden, Maassluis, Oldenzaal, Raalte, Ronde Venen, Rotterdam, Stede Broec, Enkhuizen, Drechterland, Vijfheerenlanden, Weesp en Woerden.



Figuur 2: Aantal datalekken per 10.000 inwoners

Rijswijk meldde in 2019 geen van de 20 datalekken aan de AP. De benchmarkgemeenten meldden gemiddeld 32% van de datalekken aan de AP. Bijna alle van de 24 benchmarkgemeenten meldden (ruim) meer dan 10% van de datalekken aan de AP. Slechts twee gemeenten deden in 2019 net als Rijswijk geen melding aan de AP. Resumerend heeft Rijswijk een aantal datalekken dat vergelijkbaar is met andere gemeenten, maar meldt Rijswijk beduidend minder dan andere gemeenten aan de AP.

Bevindingen:
- De gemeente houdt een register datalekken bij en heeft het beheer van datalekken op orde.
- De meldingsbereidheid en het bewustzijn over (de mogelijke impact van) datalekken neemt toe. Medewerkers en managers weten wat de procedure inhoudt en bij wie ze een datalek moeten melden.
- De organisatie duidt ongeveer de helft van de datalekken aan als menselijke fout. Wanneer de organisatie datalekken als menselijke fout en niet als systeemfout aanmerkt, bemoeilijk dat het leren en verbeteren op organisatieniveau.
- De gemeente Rijswijk meldt vrijwel geen van de geconstateerde datalekken aan de AP. Een datalek hoeft niet te worden gemeld als het niet waarschijnlijk is dat het datalek leidt tot een risico voor de rechten en vrijheden van betrokkenen.
- De gemeente Rijswijk heeft ongeveer evenveel datalekken als andere gemeenten. Rijswijk meldt echter beduidend minder datalekken aan de AP dan andere gemeenten.

Organisatiecultuur

De manier waarop de organisatie omgaat met privacy en informatiebeveiliging wordt sterk beïnvloed door informele processen, sociale factoren en de organisatiecultuur.[30] Zo blijkt in de organisatie de opvatting te heersen dat - hoe vervelend dat ook is - fouten maken menselijk is en er altijd iets mis kan

[30] AVG, Handreiking rekenkameronderzoek naar privacy in het sociaal domein 2020.

gaan. Medewerkers hebben het idee dat er geen afrekencultuur bestaat binnen het sociaal domein: ''we zijn immers een lerende organisatie''. Toch vinden sommige medewerkers het spannend en/of heerst er ''schaamte'' om een datalek te melden. Daarom besteed de privacy officer daar aandacht aan door nieuwe medewerkers uit te leggen dat fouten maken menselijk is en benadrukt zij het belang van het melden ervan.

Praktische instelling
De verwerking van gegevens in het sociaal domein vindt plaats binnen een complexe context: er is snel hulp nodig, en het gaat om gevoelige informatie. Dat brengt dilemma's met zich mee. Zo is er sprake van een spanningsveld tussen de kwaliteit van dienstverlening en (het borgen van) privacy. Daarom proberen medewerkers daar pragmatisch mee om te gaan. De vraag en afweging voor de organisatie is daarom altijd: mensen helpen of de AVG naleven.

Bevindingen:
- De gemeente besteedt aandacht aan het bewustzijn van (nieuwe) medewerkers om eventuele ''schaamte'' voor het melden van datalekken te minimaliseren. Die organisatiecultuur draagt daarmee bij aan de borging van privacy en informatieveiligheid.
- Er heerst een praktische instelling als het gaat om het borgen van privacy. De gemeente probeert een modus te vinden tussen dienstverlening en gegevensbescherming van burgers.

4.3 Training en bewustzijn van medewerkers
Medewerkers zijn belangrijke schakels op het terrein van informatiebeveiliging en privacy. Want als medewerkers niet alert zijn en de richtlijnen en tips niet volgen, kan het alsnog mislopen. Aandacht voor het bewustzijn over de risico's is dan ook essentieel. Het is een continu aandachtspunt. De gemeente besteedt daar op verschillende wijzen aandacht aan. Onder andere de CISO en privacy officer spelen een belangrijke rol bij die ontwikkeling.

Eed, belofte of geheimhoudingsverklaring
Allereerst van belang in de omgang met informatie en persoonsgegevens is dat interne medewerkers een eed of belofte afleggen waarvan geheimhouding impliciet onderdeel is. Tevens is geheimhouding geborgd in de gedragscode van de gemeente. Externe medewerkers tekenen een geheimhoudingsverklaring.[31]

Bewustwordingscampagne en Intranet (Edison)
Om te zorgen dat de privacyregels worden nageleefd organiseert het team I-bewust[32] een doorlopende bewustwordingscampagne (I-bewust). Dat houdt onder meer in dat medewerkers via Intranet blijvend geïnformeerd worden via maandelijkse berichten over beveiligings- en privacyrisico's. Verder staan er op Intranet diverse pagina's met richtlijnen voor de uitvoering zoals een pagina I-bewust, juridische informatie, een handboek sociaal domein en uitleg over de procedure voor het melden van datalekken.

[31] Jaarrapportage van de FG 2020.
[32] Bestaande uit tien personen: de CISO, de privacy officer, de privacy jurist, een medewerker communicatie, een medewerker van i-advies (team informatie), de service level manager (team informatie), iemand van de Gemeenschappelijke Regeling, een medewerker van het team Veiligheid (i.v.m. cybersecurity), iemand uit de OR en de coördinator integriteit.

Training

Nieuwe medewerkers volgen verplicht twee trainingen: AVG Security Awareness en Privacy Security Awareness via het e-learningplatform van de Rijswijk Academie.[33] Daarnaast is er een algemene AVG cursus AVG die medewerkers op vrijwillige basis kunnen volgen. Ook zijn er enkele gerichte acties en trainingen voor mensen die zich meer bezighouden met informatie en gegevensdeling. Zo is er voor alle mensen die zich bezighouden met informatiesystemen een training Privacy by Design georganiseerd. Het is de verantwoordelijkheid van de manager om ervoor te zorgen dat niet enkel nieuwe medewerkers, maar ook het vaste personeelsbestand trainingen volgt. De CISO en privacy officer proberen de managers te motiveren om de trainingen aan te bieden aan hun team.

Uit de gesprekken bleek dat de beschikbaarheid van bovengenoemde trainingen niet bij iedereen in de organisatie bekend is. Ook uit de jaarrapportage van de FG blijkt dat niet bekend is ''of op afdelingsniveau protocollen en procedures beschikbaar zijn over de wijze van omgang met persoonsgegevens en of alle medewerkers actief getraind worden om de kennis van het privacyrecht en het privacybewustzijn op het specifieke domein te verhogen''. Consulenten geven aan dat zij, naast de mogelijkheid tot wekelijks overleg, behoefte hebben aan meer training omdat hun kennis over de AVG vrij snel vervaagt. Verder zou er binnen sommige teams mogelijk verschil zitten in het aanbod van trainingen wanneer de teams (deels) bestaan uit externen vanuit verschillende organisaties. Uit de stukken is dan ook niet gebleken dat er in het bijzonder aandacht wordt besteed aan afspraken met of kennis van externen over privacy en meer specifiek het privacybeleid van de gemeente.

Kennissessies

Gemeentebreed zijn er in 2020 kennissessies gehouden. De FG, privacy officer en privacy jurist hebben eerder aan alle teams in het sociaal domein (bijv. Wmo, schuldhulpverlening en Participatie) uitleg gegeven over wat de AVG inhoudt. In 2020 is er geen (herhaal)presentatie gehouden in de teams. Vanaf 2021 is het de bedoeling om dat wel te doen en te blijven herhalen. Daarnaast wil de senior adviseur Kwaliteit voor de teams jaarlijks leerbijeenkomsten organiseren waarin casuïstiek wordt besproken.[34] In het eerste kwartaal van 2021 heeft de senior adviseur Kwaliteit gesproken met alle teamleiders over de vraagstukken die leven op het gebied van de AVG en privacy. Uit die gesprekken bleek dat bij met name het Sociaal wijkteam en het Jeugdteam privacygerelateerde vragen leven die te maken hebben met de uitoefening van hun werk.

Testen van bewustzijn

Team I-bewust toetst het bewustzijnsniveau van de medewerkers door het uitvoeren van jaarlijkse phishingmail simulaties, werkplekonderzoeken en tests met een mystery guest. De resultaten van de tests en onderzoeken worden gedeeld binnen de organisatie om medewerkers alert te houden. Gemeentebreed blijken nog relatief veel mensen in de phishingmails te trappen.

[33] Een van de verplichte overheidsmaatregelen in de BIO is dat nieuwe medewerkers binnen drie maanden na aanstelling een training moeten doorlopen op dit gebied.

[34] Deskundigheidsbevordering en het geven van presentaties is dan ook onderdeel van de borging AVG.

Ten behoeve van de jaarlijkse DigiD-audit wordt er een pentest uitgevoerd. Daarnaast wordt er in samenwerking met de gemeente Delft jaarlijks een extra audit uitgevoerd op een specifiek onderdeel. In 2020 is aan externe onderzoekers gevraagd om op basis van het scenario van de hack bij de universiteit van Maastricht de beveiligingsmaatregelen bij de GRB Delft-Rijswijk te testen.

De bewustwording over privacy binnen de organisatie is een doorlopend en herkenbaar verbeterpunt in Rijswijk. Zo zou er meer bewustwording moeten zijn over (het effect van) datalekken, omdat er nog steeds medewerkers zijn die niet weten wat een datalek is of het niet herkennen. Verder wordt genoemd dat er sprake is van een goed bewustzijnsniveau als het gaat om het herkennen van persoonsgegevens en de bescherming daarvan, maar dat er nog stappen te maken zijn als het gaat om de toepassing van de AVG en de bewustwording in het herkennen en erkennen van grondslagen die van toepassing zijn. Dat gaat over vragen als ''wanneer is toestemming nodig?''. Desondanks worden medewerkers steeds meer bewust en bekwaam, en is er merkbaar progressie bij de gemeente Rijswijk, aldus verschillende gesprekspartners.

Bevindingen:
- Er sprake van een reeks aan acties, trainingen en opleidingstrajecten om kennis en bewustzijn over het belang van privacy en informatieveiligheid te borgen.
- In het sociaal domein hebben sommigen behoefte aan meer training over de AVG.
- Het lijnmanagement is verantwoordelijk voor het aanbieden van trainingen, maar wijst medewerkers onvoldoende op de beschikbaarheid en het nut van trainingen op het gebied van privacy.
- Kennis, bewustzijn en training van externe medewerkers is een aandachtspunt.

4.4 Organisatie in het sociaal domein

Het sociaal domein bestaat uit de volgende teams: het Financieel Servicepunt (FSP), team Werk, team Inkomen, team Wmo, het Jeugdteam en het Sociaal wijkteam. Sommige teams hebben een teamleider en daarboven staat er een sociaal domein-manager. Aan ieder team is een kwaliteitscoach verbonden die gespecialiseerd is in het werkveld van het team en aandacht besteed aan het opstellen, evalueren en bewaken van de processen.[35] De kwaliteitscoach biedt de consulenten begeleiding en deskundigheidsbevordering. Aanvullend is er bij het Sociaal wijkteam en Jeugdteam ook een gedragswetenschapper beschikbaar.

Op het moment dat de kwaliteitscoach er niet uitkomt, ruggespraak wil of vindt dat er iets moet gebeuren in het proces, komt de kwaliteitscoach bij de senior adviseur Kwaliteit. Indien nodig en waar mogelijk wordt het proces en/of de instructie dan aangepast. De kwaliteitscoach en senior adviseur Kwaliteit kijken dan samen naar het onderwerp. Daarnaast overleggen zij regelmatig met elkaar over wat er speelt op de werkvloer. Een vraag die regelmatig voorbij komt, is een casuïstiek vraag zoals ''mag ik gegevens delen met'' een andere partij of collega bijvoorbeeld, en zo ja, ''hoe moet ik dat doen''.

[35] De kwaliteitscoach is in dienst van de gemeente.

In het geval van privacy gerelateerde vragen of dilemma's kunnen consulenten in eerste instantie terecht bij de kwaliteitscoach of gedragswetenschapper van het team. De kwaliteitscoach is de vraagbaak voor procesmatige vragen. De gedragswetenschapper is er vooral voor casusinhoudelijke vragen en moet betrokken worden bij het maken van kernbesluiten, bijv. de stap naar de Jeugdbeschermingstafel.[36] Daarnaast kunnen consulenten ook zelf met privacy vragen terecht bij de senior adviseur Kwaliteit die zich bezighoudt met de AVG.

Het Jeugdteam heeft wekelijks overleg met de gedragswetenschapper waarin casussen kunnen worden besproken en vragen kunnen worden gesteld. Het thema privacy komt niet specifiek naar voren in ieder werkoverleg; dat verschilt per team. Vragen of problemen omtrent privacy spelen minder bij het FSP. Wanneer een inwoner een aanvraag doet bij het FSP geeft de inwoner vooraf toestemming dat het FSP bij bijvoorbeeld schuldeisers mag informeren.

De consulenten zijn bekend met het privacybeleid en de procedure voor het melden van datalekken. Beiden denken dat de procedure goed werkt en het goed wordt opgepakt door collega's en leidinggevende. Na een datalek stuurt de leidinggevende een mail met de reminder om goed op te letten en welke stappen nodig zijn om een datalek te voorkomen. Datalekken komen volgens de geraadpleegde consulenten niet vaak voor bij het FSP en het Jeugdteam. Zij hebben het over een à twee keer in de jaren dat zij werkzaam zijn bij de gemeente.

Verder blijkt uit de gesprekken dat wanneer consulenten vragen hebben over privacy, zij dat vrij gemakkelijk kunnen opzoeken. Zo werkt de gemeente met een kwaliteitshandboek met processen en procesbeschrijvingen dat op intranet staat. Ook hebben alle consulenten toegang tot Schulinck waar ter ondersteuning ook vragen kunnen worden gesteld.[37] In Schulinck is ook een onderdeel privacy opgenomen met (landelijk) veel gestelde vragen. Een landelijk veel gestelde vraag is bijv. ''mag ik informatie delen met een collega?''. Verder is het voor de consulenten gebruikelijk om een mail te sturen of te bellen naar de kwaliteitscoach of gedragswetenschapper bij vragen; daar komt over het algemeen snel antwoord op. De consulenten ervaren daar steun aan.

Toezicht en controle

De kwaliteitscoaches nemen dossiers door en doen de eerstelijns toetsing daarvan. Zodoende kunnen zij verbeterpunten signaleren. Dat gaat niet enkel over de AVG, maar ook over andere vraagstukken. Bij Kwaliteit wordt er ook een tweedelijns toetsing gedaan. Vanuit hun onafhankelijke positie wordt een steekproef gedaan om te kijken of medewerkers hun werk op een goede manier uitvoeren. Vaak gaat dat over de inhoud – zoals de beoordeling - maar eventuele verbeterpunten kunnen ook gaan over de omgang met privacy(regels).

Intervisie en begeleiding voor consulenten

De gemeente faciliteert intervisie en inhoudelijke begeleiding voor medewerkers. Intervisie is bedoeld voor (anonieme) bespreking van alle casussen waarin medewerkers dilemma's ervaren. Een complex

[36] Dit is hoe de functies van kwaliteitscoach en gedragswetenschapper er binnen het Jeugdteam uitzien.
[37] Schulinck is een online, juridische kennisbank die betrekking heeft op onder meer het sociaal domein binnen gemeenten.

privacy dilemma kan ook een vraagstuk voor intervisie zijn.[38] Zodoende kunnen consulenten op casuïstiek niveau overleggen met een kwaliteitscoach en/of een gedragswetenschapper.

[38] Denk aan een medewerker met beroepsgeheim die tijdens intervisie met collega's die ook een beroepsgeheim hebben, kan overleggen over hoe dat gaat.

Samenwerking

Afspraken over gegevensverwerking en uitwisseling met derden of uitbesteding van taken dienen in juridische documenten vastgelegd te worden zoals convenanten en verwerkersovereenkomsten. De gemeente maakt daar aantoonbaar gebruik van. De privacyjurist toetst de rechtmatigheid van de documenten. Nog niet alle afspraken zijn vastgelegd. Momenteel wordt er gewerkt aan de samenwerking tussen het Jeugdteam, het FSP en het Sociaal wijkteam waarbij ook gekeken wordt naar hoe dat privacytechnisch goed kan worden ingebouwd.[39]

Bevindingen

- Consulenten kunnen casussen waarin zij privacydilemma's ervaren anoniem bespreken met een kwaliteitscoach, gedragswetenschapper of de senior adviseur Kwaliteit. Ook kunnen zij deze voorleggen tijdens intervisie.
- De ambtelijke organisatie probeert privacy zo veel als mogelijk te borgen in convenanten, overeenkomsten en afspraken.

[39] Daarin wordt onder andere aangegeven dat als er een inwoner - met bijv. een ontruiming - zich meldt bij het Sociaal wijkteam, dat het Sociaal wijkteam dan ook toestemming vraagt om de gegevens van de ontruiming met het FSP te delen.

5. Communicatie met inwoners

De AVG bepaalt dat de gemeente een informatieplicht heeft ten opzichte van haar burgers. Dat betekent dat wanneer burgers om een dienst vragen en de gemeente gegevens verzamelt van hen, de gemeente verplicht is om burgers duidelijk te informeren over wat de gemeente met hun persoonsgegevens doet en waarom. Ook is in sommige gevallen toestemming nodig van burgers om gegevens te mogen delen met derden. Daarom staat de volgende vraag in dit hoofdstuk centraal:

- Hoe communiceert de gemeente naar inwoners over de wijze waarop zij omgaat met persoonsgegevens?

Website

De AP geeft aan hoe in de praktijk het handigst kan worden voldaan aan de informatieplicht: ''In de AVG staat dat u de informatie over uw verwerkingen in principe schriftelijk moet geven. De beste manier om er zeker van te zijn dat uw informatie voor de meeste mensen goed vindbaar is, is het publiceren van een online privacyverklaring''.[40] Veel gemeenten hebben dan ook een privacyverklaring op hun website gepubliceerd. De website vermeldt wel informatie over 'privacy', maar de gemeente duidt dat niet als privacyverklaring.[41] Er is een pagina over het toezicht op gegevensbescherming met informatie over de FG en de AP, een pagina waarop de rechten van betrokkenen uiteen worden gezet en wordt uitgelegd hoe inwoners hun rechten kunnen uitoefenen.[42] Voorbeelden van ''rechten van betrokkenen'' zijn het recht op informatie, het recht op inzage en het recht van bezwaar.[43] Burgers kunnen hun privacyrechten laten gelden met behulp van een digitaal formulier op de website. Het proces van afhandeling van dergelijke verzoeken werkt via DigiD zodat mensen zich digitaal kunnen identificeren. Ook is er een pagina voor het melden van datalekken en bestaat de mogelijkheid voor burgers om de FG te contacteren. Aanvragen voor de FG komen meestal per mail binnen. Dat komt niet veel voor. Afhankelijk van de vraag wordt dat per mail of telefonisch beantwoord.

Intakegesprekken

De consulenten van het Jeugdteam vragen bij de intake standaard toestemming aan ouders om gegevens op te vragen bij - en te delen met - andere partijen. Die toestemming hebben ze altijd nodig. Het Jeugdteam is transparant naar ouders en geeft hen ook terugkoppeling na opvraag van gegevens. Verder wordt inwoners verteld dat de toestemming weer ingetrokken kan worden.

Toestemming vragen aan betrokkenen - als grondslag voor het verwerken of delen van gegevens - kan niet zomaar.[44] Gemeenteambtenaren bevinden zich in een machtspositie ten opzichte van de inwoner. Toestemming moet vrij en specifiek gegeven kunnen worden. Daar moeten consulenten over nadenken. Transparantie is daarbij belangrijk. Wanneer er gegevens worden gedeeld moet dit altijd besproken worden met de inwoner. Uit de gesprekken is gebleken dat consulenten wel toestemming vragen wanneer het delen van gegevens in het belang van de cliënt is - en de zorgplicht van de

[40] zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/rechten-van-betrokkenen#is-een-privacyverklaring-volgens-de-avg-verplicht-6253
[41] https://www.rijswijk.nl/over-deze-website
[42] De verzoeken in het kader van de rechten van betrokkenen zijn bijgehouden in het jaarverslag van de FG.
[43] Zie ook: https://www.rijswijk.nl/uw-recht-op-privacy.
[44] In april 2016 publiceerde de Autoriteit Persoonsgegevens (AP) het rapport Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming. De AP gaf daarin aan dat toestemming in het sociaal domein niet rechtsgeldig zal zijn. Dit vanwege de afhankelijke relatie waarin de cliënt ten opzichte van de gemeente staat. Deze afhankelijke situatie maakt dat toestemming niet in vrijheid gegeven zal zijn.

gemeente dus een rol speelt - en consulenten goed uitleggen waarvoor het opvragen en delen van informatie nodig is. Soms vragen consulenten toestemming op momenten dat het (mogelijk) niet nodig is. Omdat er in de praktijk soms vragen over bestaan, zal de gemeente in 2021 aandacht besteden aan het onderwerp “toestemming” tijdens de voorlichting van de teams.

Werkwijze en navolgbaarheid van toestemming
Het FSP werkt met een toestemmingsformulier voor het opvragen van informatie. Het Jeugdteam werkt niet meer met schriftelijke toestemmingsformulieren, maar met mondelinge toestemming of toestemming per mail. Ten behoeve van ‘’rechtmatigheid, behoorlijkheid en transparantie”[45] is het van belang dat het besluitvormingsproces navolgbaar is. In het geval van mondelinge toestemming is de toestemming niet navolgbaar. Op het moment dat bijvoorbeeld de GGZ de toestemming schriftelijk wil ontvangen, moet het Jeugdteam dan ook weer achter de schriftelijke toestemming van de ouder(s) aan.

Dossierinzage
Het Jeugdteam rapporteert over de jeugdige. Enkel mensen uit het Jeugdteam hebben toegang tot het dossier. Ook ouders hebben zelf nog geen toegang tot dossiers. Ouders kunnen een dossieropvraag doen. Dat verloopt via de leidinggevende die een eerste controle doet op welke informatie uit het dossier wel en niet met de ouder kan worden gedeeld. Informatie waar twijfels over bestaan, controleert de leidinggevende bij de consulent.

Dilemma’s
De gemeente wil integraal (of domeinoverstijgend) samenwerken, maar integraal gegevens delen – denk aan werken vanuit het principe van één gezin, één plan – is lastig. De grondslag voor het delen van gegevens ontbreekt vaak waardoor de gemeente tegen de grenzen van de privacyregels aanloopt. Uitvoeringsprofessionals stuiten dagelijks op ethische dilemma’s: voldoen aan de AVG of gegevens uitwisselen om mensen te helpen? In afwachting van de Wet aanpak meervoudige problematiek sociaal domein (Wams) worden gegevens vaak gedeeld op basis van toestemming van de betrokkene. Integraal werken brengt tot die tijd mogelijk privacyrisico's met zich mee in de zin van dat er te veel gegevens worden gevraagd, opgeslagen en/of gedeeld. Met name voor inwoners die niet zelfredzaam zijn, moet gekeken worden naar de inrichting van het proces, zodat integraal werken mogelijk wordt. De gemeente besteedt daar aandacht aan door te werken aan beleid, heldere werkprocessen en aan het versterken van kennis en expertise van medewerkers. Zoals eerder genoemd, gaan de senior adviseur Kwaliteit en de privacy officer vanaf juni 2021 een leergang ‘’organiseren van privacy’’ van de VNG volgen zodat privacy en gegevensdeling bij deze groep cliënten dusdanig kan worden georganiseerd dat consulenten optimaal ondersteund worden bij omgaan met privacy dilemma's.

De gesprekspartners schetsen een wisselend beeld van de (intake)gesprekken met burgers. Zo geeft de privacy officer aan dat consulenten tijdens de (soms moeilijke) gesprekken die zij voeren, eigenlijk niet ook nog het AVG verhaal willen aankaarten. Ook de portefeuillehouder sociaal domein denkt dat het soms lastig kan zijn voor consulenten. De wethouder spreekt veel medewerkers in de uitvoering van het sociaal domein en hoort vaak dat de AVG meer tegenwerkt dan dat het medewerkers helpt in de uitvoering. Zo moet er vaak toestemming worden gevraagd voor het delen van gegevens. Voor

[45] Zoals een van de AVG-beginselen luidt.

burgers is dat ook vervelend. Het is lastig uitleggen waarom gegevensdeling niet zomaar mag en dat burgers veel verschillende formulieren moeten invullen als het gaat over informatieverstrekking aan derden. Mogelijk creëert de gemeente als overheidsorgaan een soort wantrouwen bij burgers die bijvoorbeeld vaker hun verhaal moeten vertellen. Toch geven de consulenten de indruk dat het geen obstakel vormt. Zo lang zij transparant zijn en inwoners zo veel mogelijk meenemen in het proces - ook wat betreft privacy - komen ze een heel eind samen met inwoners.

Bevindingen:

- De gemeentelijke website bevat informatiepagina's over privacy, de rechten van betrokkenen, het melden van datalekken etc. De gemeente duidt deze informatie niet als privacyverklaring.
- In het zorg- en veiligheidsdomein wordt de AVG soms als beperkend ervaren, bijvoorbeeld bij het delen of ontvangen van informatie in de samenwerking met derden.
- Integraal werken brengt privacyrisico's met zich mee, met name in het geval van inwoners die niet zelfredzaam zijn.
- Consulenten zijn transparant naar burgers. Zij zijn zich er bewust van dat ze burgers moeten informeren en meenemen in wat zij doen met hun gegevens.
- Bij het Jeugdteam werkt men uitsluitend met mondelinge toestemming, waardoor de registratie daarvan tekortschiet en de toestemming niet navolgbaar is.
- Toestemming vragen is niet altijd nodig en wenselijk. Wanneer consulenten 'onnodig' toestemming vragen, kan dat ten koste gaan van de integrale benadering en de dienstverlening.

6. Risico's en borging privacy

De gemeente Rijswijk heeft dus procedures, werkinstructies, verschillende registers en zet in op kennis en opleiding. Het werken met persoonsgegevens is echter altijd risicovol, zo geven gesprekspartners aan. Daarom staat dit hoofdstuk in het teken van de risico's in de huidige werkwijze voor het borgen van privacy:

- Welke mogelijke risico's zijn te onderkennen in de huidige wijze waarop de privacy van de inwoners is geborgd binnen de gemeente?
- Hoe ziet de gemeente erop toe dat de borging van de privacy van een voldoende niveau is en blijft en wordt er geanticipeerd op toekomstige opgaven en juridische ontwikkelingen?

6.1 Mogelijke risico's

De jaarrapportage van de FG is het resultaat van de zelfevaluatie. Daaruit volgen enkele knelpunten die, op enkele uitzonderingen na, voor alle domeinen gelden: het bevorderen van AVG-kennis en bewustwording over privacy, het tijdig melden en afhandelen van datalekken, het goed administreren van de verwerkersovereenkomsten, het vooraf in kaart brengen van privacyrisico's (middels het uitvoeren van DPIA's), het toepassen van de principes van privacy by design etc. Het melden van datalekken, het uitvoeren van DPIA's en het sluiten van verwerkersovereenkomsten zouden dan ook door een deel van de organisatie als procesbelemmerend worden gezien.[46]

Gesprekspartners geven aan dat datalekken moeilijk beheersbaar zijn. Door mensen op de werkvloer te instrueren en managers te wijzen op het belang van (tijdig) melden, is daar aandacht voor. Zoals eerder genoemd, probeert de gemeente het bewustzijn (onder meer) te testen en mensen alert te houden door het uitvoeren van verschillende tests en simulaties.

Door het uitvoeren van een DPIA worden privacyrisico's vooraf in kaart gebracht. Het uitvoeren van DPIA's kost extra tijd. Wanneer er sprake is van tijdsdruk, blijkt dat niet iedereen in de organisatie blij is met het moeten uitvoeren van een DPIA. Daarom wordt het soms als procesbelemmerend ervaren. De privacy officer en CISO ondersteunen daar bij en adviseren over de risicobeperkende maatregelen. Zij proberen momenteel het bewustzijn binnen de domeinen te bewerkstelligen. Dat het bewustzijn beter kan, raakt ook aan het ''volwassenheidsniveau'' van het procesmanagement. Dat houdt in dat men weet welke processen hij onder z'n hoede heeft, het besef dat men daarin een rol heeft als proceseigenaar en het begrip wat er van de proceseigenaar verwacht wordt. Het is van belang dat de proceseigenaar constant een risicoafweging maakt bij het proces.[47]

Het sluiten van verwerkersovereenkomsten wordt als steeds normaler en logischer gezien. Dat heeft deels te maken met de kennis van leveranciers van applicaties en diensten. Zodoende worden medewerkers er niet meer mee verrast.

Bij aanschaf van nieuwe applicaties letten de privacy officer en CISO erop dat de principes van Privacy by Design worden opgenomen. Dat houdt bijvoorbeeld in: het inbedden van de actieve informatieplicht aan burgers in het proces, dat niet meer gegevens worden vastgelegd dan nodig is,

[46] Gemeente Rijswijk, jaarrapportage van de FG, 2020.
[47] Niet enkel wat betreft privacy en informatiebeveiliging, maar ook wat betreft politieke gevoeligheid, continuïteit, leveranciersafhankelijkheid etc. Daarop moet de proceseigenaar altijd alert zijn op moment dat er iets verandert in het proces.

dat gegevens vernietigd worden na het verloop van de bewaartermijnen en alleen bevoegde personen toegang krijgen tot persoonsgegevens. De aandacht voor Privacy by Design begint ook in het sociaal domein nu te ontstaan.

Verbetercyclus
Naar aanleiding van het jaarrapport van de FG en de verbeteracties die daaruit voort kwamen, heeft de FG voor het management een (online) presentatie gegeven, zodat de managers de verbeterpunten binnen de teams kunnen verspreiden. Tijdens de sessie is het management in vier groepen verdeeld die werden begeleid door de CISO, de privacy officer, het hoofd JZ en de FG. Als er bepaalde zaken structureel fout gaan bij hetzelfde team, moet de leidinggevende een gesprek gaan voeren met zijn team. Het is immers de verantwoordelijkheid van het lijnmanagement om incidenten zoals datalekken te bespreken in werkoverleggen en in het vervolg te voorkomen. De privacy officer en CISO wijzen de managers daar op en bieden aan om daarover mee te denken. Zij kunnen echter niet goed inschatten of dat daadwerkelijk door managers wordt opgevolgd.
De privacy officer en senior adviseur Kwaliteit bespreken af en toe de datalekken zodat zij samen kunnen kijken naar eventuele verbetering en aanpassing van processen. Verder is het de bedoeling dat privacybescherming een onderdeel wordt van het functionele beoordelingsgesprek voor functies waar privacybescherming een issue kan zijn.[48] Toch wordt ook de kanttekening gemaakt dat de gemeente - en organisaties in het algemeen - vooral leert van grote incidenten waarbij zij bijvoorbeeld financiële en/of imagoschade lijdt.

Auditresultaten
In de audit van de accountant (najaar 2020) kwam onder meer naar voren dat de databases voor WMOned, Key2Financiën en Suites voor het sociaal domein niet zijn voorzien van passende wachtwoordeisen. De gemeente werd dan ook geadviseerd de wachtwoordeisen aan te scherpen daar het een verhoogd risico tot ongeautoriseerde toegang oplevert.[49] Uit de gesprekken bleek dat wachtwoordvereisten en het regelmatig wijzigen van bijv. wachtwoorden wel als ''moeilijkheden'' in de werkbaarheid werden gezien en daardoor een mogelijk risico kan vormen. Denk aan wanneer medewerkers om de regels gaan heen werken.

Verder werd aangeraden om twee-factor authenticatie niet alleen voor extern inloggen, maar ook voor intern inloggen bij gemeentelijke kantoren (''alle locaties'') door te voeren zodat het risico op ongeautoriseerde inlogpogingen wordt verlaagd.

Daarnaast bleek er geen organisatie brede functie-autorisatiematrix beschikbaar te zijn. De accountant raadde daarom aan om een functie-autorisatiematrix op te stellen en deze te gebruiken als basis voor de toekenning van autorisaties binnen de verschillende applicaties. Verder ontstaat er daarmee een norm waaraan accounts kunnen worden getoetst. Verschillende gesprekspartners geven aan dat de gemeente inmiddels bezig is met het controleren van autorisaties en autorisatieschema's.[50]

[48] Dit wordt wel al gedaan in bijv. de gemeente Amersfoort; zie het recent verschenen rapport van de Rekenkamer Amersfoort over de bescherming van persoonsgegevens, 2021.
[49] Baker Tilly, Managementletter gemeente Rijswijk 2020.
[50] Baker Tilly, Managementletter gemeente Rijswijk 2020.

Bevindingen:

- De gemeente heeft inzichtelijk welke risico's er momenteel bestaan. De FG signaleert verbeterpunten in zijn jaarverslag, waarmee de organisatie probeert te leren en verbeteren.
- Het bewustzijn over de noodzaak en vanzelfsprekendheid van acties om risico's zoveel als mogelijk te beperken, is een verbeterpunt.
- 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.
- Risico's die de accountant constateert, betreffen de wachtwoordvereisten, twee factor-authenticatie en de functieautorisatiematrix.

6.2 Toekomstige opgaven en juridische ontwikkelingen

In het informatiebeleidsplan 2020-2022 (IBP) formuleert de gemeente een visie voor de informatievoorziening bij de gemeente Rijswijk.[51] Een van de uitgangspunten van het (strategisch) informatiebeleid is informatieveiligheid en privacy. De gemeente Rijswijk heeft in het kader daarvan aandacht voor (toekomstige) ontwikkelingen als consumerization[52] en ATAP-werken[53]. De grenzen van de gemeentelijke organisatie vervagen en cybercriminaliteit is een risico. De gemeente Rijswijk streeft daarom onder meer naar het aanwijzen van verantwoordelijken voor gegevens en applicatiefuncties, de toegang tot gevoelige gegevens in de applicaties die persoonsgegevens bevatten te loggen en te beoordelen, informatiebeveiliging te borgen in afspraken etc.[54] Uit de gesprekken blijkt dat er op dit moment nog niet in alle domeinen verantwoordelijken zijn aangewezen en er onvoldoende capaciteit is om bepaalde verbeterpunten op te pakken zoals het loggen van de toegang tot gegevens.

Beveiligd communiceren met inwoners

Het beveiligd communiceren met burgers - zoals de beveiligde mail - is niet altijd gebruiksvriendelijk. Het risico is dan ook dat de gebruikersvriendelijkheid van de oplossing belemmerend werkt voor het gebruik daarvan en burgers dus op een onveilige manier hun informatie delen.

Thuiswerken

Rijswijk heeft de benodigde techniek voor het thuiswerken op orde en test het systeem regelmatig. De gemeente heeft een jaar voordat het thuiswerken noodzakelijk werd een risicoanalyse gedaan op het telewerken. De gemeente hanteert een protocol telewerken en heeft veel energie gestoken in het bekendmaken van het protocol bij medewerkers. Een belangrijk onderdeel daarvan gaat over gedrag. In dat protocol staat dan ook beschreven hoe verwacht wordt dat mensen met informatie omgaan wanneer ze niet op kantoor zijn. Zo moeten medewerkers ervoor zorgen dat ze in een gecontroleerde omgeving zitten. Dat geldt voor zowel de fysieke als technische omgeving. De technische omgeving

[51] Gemeente Rijswijk, Informatiebeleidsplan 2020-2022.

[52] Rijswijk beschrijft de ontwikkeling van consumerization als volgt: ''Mensen zijn steeds meer ervaren IT gebruikers en willen zelf bepalen welke apparatuur en applicaties ze gebruiken. Mobiele telefoons, tablets en notebooks zijn een normaliteit geworden en mensen willen ze graag overal mee naartoe kunnen nemen en gebruiken (Bring Your Own Device). Veel applicaties zijn gratis op Internet beschikbaar en sluiten beter aan bij behoeften dan formele werkplekken''.

[53] ATAP staat voor any time any place. De ontwikkeling van ATAP-werken wordt door Rijswijk beschreven als: ''Mensen willen steeds meer werken op het tijdstip en de plaats waarop het hen het beste uitkomt. Dit is een kernonderdeel van Het Nieuwe Werken, waarbij voor verschillende werkzaamheden ook verschillende werkomgevingen worden gebruikt. Dat kan zijn overdag op kantoor, onderweg of 's avonds thuis''.

[54] Gemeente Rijswijk, Informatiebeleidsplan Rijswijk 2020-2022.

betreft een beveiligde verbinding die tot stand wordt gebracht met een token waarmee men inlogt in het systeem. Omdat medewerkers dan werken op het systeem van de gemeente, blijft er niets achter op het apparaat. Het wifi netwerk dat medewerkers gebruiken heeft dan ook niet meer zo veel invloed. Er wordt naar medewerkers gecommuniceerd dat ze binnen de gecontroleerde, beveiligde omgeving moeten werken en enkel daarbinnen hun informatie moeten opslaan.

Papierloos werken

De gemeente werkt nog niet volledig papierloos. Omdat alles dat wordt afgedrukt een extra risico vormt, worden medewerkers gevraagd om zo min mogelijk af te drukken. Nadat uit het werkplekonderzoek bleek dat men soms nog documenten achterliet op de bureaus, werd weer benadrukt dat het niet de bedoeling is. De CISO vermoedt dat nu iedereen thuiswerkt, medewerkers nog meer digitaal werken en dus ook minder documenten printen.

Bevindingen

- De gemeente heeft een visie als het gaat om toekomstige opgaven voor privacy en informatieveiligheid.
- Met het oog op toekomstige ontwikkelingen en opgaven is de beperkte capaciteit een aandachtspunt.
- Het beveiligd communiceren met inwoners is een aandachtspunt.
- Thuiswerken is goed geregeld. De gemeente focust op het gedrag van medewerkers door een protocol telewerken te communiceren binnen de organisatie.

7. Sturing en controle

In dit hoofdstuk wordt ingegaan op de wijze waarop de gemeenteraad wordt geïnformeerd over privacy en informatiebeveiliging, en op de mate waarin dit handvatten biedt om invulling te geven aan zijn kaderstellende en controlerende rol. Daarmee wordt een antwoord geformuleerd op de volgende onderzoeksvragen:

- Op welke wijze is de raad tot nu toe bij de ontwikkeling van het privacybeleid en informatieveiligheid in het sociaal domein betrokken geweest?
- Op welke manier kan de gemeenteraad het beleid rondom privacy en informatieveiligheid in het sociaal domein controleren en sturen?

Het college heeft het privacybeleid en het privacyreglement vastgesteld. De raad heeft het informatiebeleidsplan 2020-2022 vastgesteld.

Privacy en informatieveiligheid wordt in de praktijk gezien als een bedrijfsvoeringskwestie. De wethouder P&O en bedrijfsvoering ontvangt via het GMT informatie over informatiebeveiliging, ICT en de AVG. De portefeuillehouder sociaal domein wordt niet geïnformeerd over specifiek dit thema. Omdat het als bedrijfsvoeringskwestie wordt gezien en de beleidsvrijheid beperkt is, komt het onderwerp maar beperkt aan de orde in het college. Het is aan de ambtelijke organisatie - en meer specifiek aan het GMT - om ervoor te zorgen dat dit thema goed geborgd wordt. Door middel van de jaarrapportage legt de FG verantwoording af aan het GMT. Het GMT stelt stukken vast en legt de stukken ter instemming voor aan het college. Het college van B&W is politiek verantwoordelijk voor het bewerkstelligen van een passend niveau van informatiebeveiliging en gegevensbescherming.[55]

Het college legt vanaf 2017 jaarlijks verantwoording af aan de raad via de paragraaf Bedrijfsvoering in de jaarrekening (dus de reguliere P&C-cyclus). Voor de verantwoording over informatieveiligheid is landelijk een eenduidige systematiek ontwikkeld (ENSIA: eenduidige normatiek single information audit). In feite wordt met de ENSIA verantwoording afgelegd over de mate waarin de BIO is geïmplementeerd. De ENSIA begint ieder jaar met een zelfevaluatie waarin ruim 300 vragen beantwoord worden. Aan de hand van de beantwoording van die vragen wordt duidelijk welke maatregelen van de BIO voldoende zijn ingevoerd en welke maatregelen nog om aandacht vragen. Daar stelt het Gemeentelijk Managementteam vervolgens een actieplan voor vast.[56] Op basis van de uitkomsten van de ENSIA wordt voor de verantwoording over het gebruik van specifiek Suwinet en de DigiD-aansluitingen jaarlijks een collegeverklaring opgesteld. De gemeenteraad wordt hierover geïnformeerd via een raadsinformatiebrief. Verder wordt de raad ook ingelicht over het aantal datalekken.

Naast de jaarlijkse verantwoording heeft de CISO eerder een bijeenkomst georganiseerd voor de auditcommissie waarvoor ook alle andere raadsleden waren uitgenodigd.[57] Tijdens de bijeenkomst heeft de CISO het informatieveiligheidsbeleid en het informatiebeveiligingsplan toegelicht en uitgelegd hoe er wordt gerapporteerd in de jaarrekening. De auditcommissie wordt eigenlijk gebruikt

[55] Gemeente Rijswijk, Informatiebeveiligingsbeleid 2020.
[56] Gemeente Rijswijk, Informatiebeveiligingsbeleid 2020.
[57] De auditcommissie bestaat uit enkele raadsleden en adviseert over en bereidt de besluitvorming in de raad voor op het gebied van de kaderstelling en controle inzake de gemeentefinanciën.

als voorportaal van de gemeenteraad, zo blijkt uit de gesprekken. De afspraak met de auditcommissie is dat er aan de bel wordt getrokken, wanneer dat nodig is.

Het thema privacy en gegevensbescherming leeft met name bij de raad wanneer er een grote verandering of (elders in Nederland) een incident heeft plaatsgevonden. In de periode 2018 tot april 2021 zijn er slechts een aantal momenten aan te wijzen dat er raadsvragen werden gesteld of er aandacht werd gevraagd voor dit thema.[58] Denk aan het moment dat de AVG net in werking trad in 2018 en toen er begin 2021 sprake was van een groot datalek bij de GGD.

Uit de gesprekken blijkt dat het college de raad meer zou moeten meenemen in het thema privacy en informatieveiligheid. Het college en de raad hebben elkaar nodig om kaders te stellen, zodat de raad het college goed kan sturen en controleren. En dat gebeurt momenteel weinig.

Bevindingen:

- De raad is betrokken geweest bij de ontwikkeling van het informatiebeleidsplan 2020-2022, maar de rol van de raad bij de ontwikkeling van het privacy- en informatiebeveiligingsbeleid is beperkt.
- Het borgen van privacy en informatieveiligheid wordt gezien als een bedrijfsvoeringskwestie. Enerzijds mag de raad verwachten dat het college de borging goed organiseert. Anderzijds dient de raad hier ook op toe te zien
- Het college neemt de raad weinig mee in het thema privacy en informatieveiligheid. Mede daardoor wordt de raad niet in staat gesteld om te sturen en controleren op dit thema.

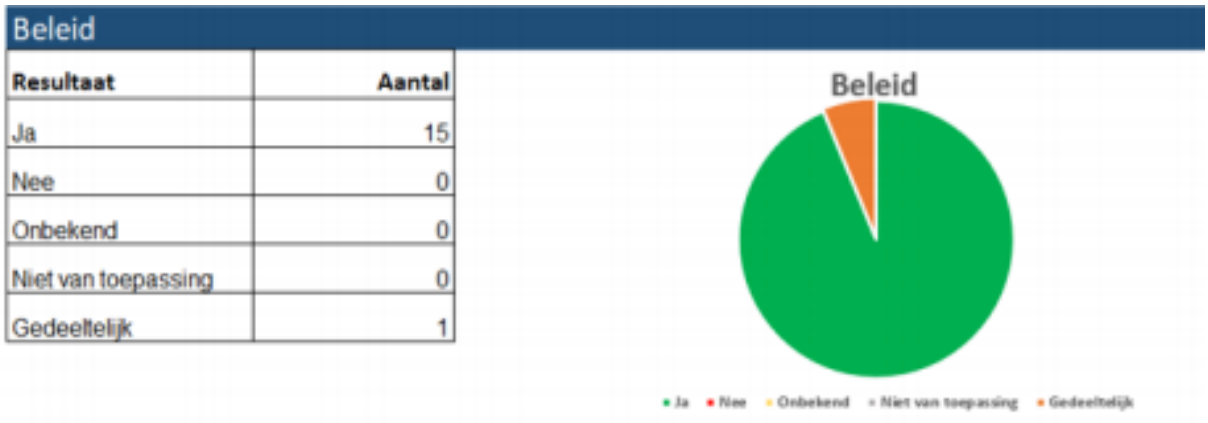
[58] Zie bijv. de vragen van respectievelijk Groenlinks en D66: ‘’Verzoek om informatie ex artikel 42 van het Reglement van Orde’’, 1 maart 2018; en ‘’ICT-en privacyproblemen bij de GGD Haaglanden’’, 2 februari 2021.

Bijlage 1. Geraadpleegde personen

- Remon Klop, manager bedrijfsvoering sociaal domein
- Marleen de Bie, senior adviseur kwaliteit en bedrijfsvoering
- Alex Tilli, functionaris gegevensbescherming
- Piera Cherchi, privacy officer
- Peter van de Vaate, CISO
- Sandy Westenbroek, jeugdconsulent
- Mendy Wijsman, senior consulent bij het financieel servicepunt (FSP)
- Larissa Bentvelzen, wethouder sociaal domein

Bijlage 2. Stand van zaken AVG per onderwerp[59]

In het document 'Het borgen van de Algemene Verordening Gegevensbescherming in de gemeentelijke organisatie' van de Informatiebeveiligingsdienst worden per onderdeel vragen gesteld of bepaalde taken (deels) zijn gerealiseerd. De cirkeldiagrammen geven per onderwerp op thema een beeld weer van in hoeverre de gemeente deze criteria heeft geïmplementeerd.

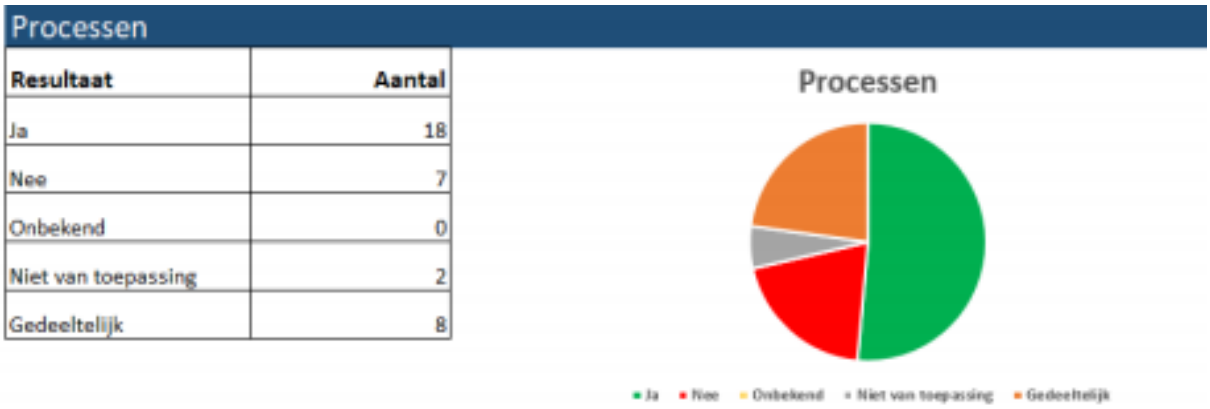


Beleid

Resultaat	Aantal
Ja	15
Nee	0
Onbekend	0
Niet van toepassing	0
Gedeeltelijk	1

Toelichting

De vereiste beleidsproducten voor de implementatie van de AVG zijn gerealiseerd. Het is zaak om bij de domeinspecifieke werkprocessen ook rekening te houden met de privacyregels uit de sectorwetgeving.



Processen

Resultaat	Aantal
Ja	18
Nee	7
Onbekend	0
Niet van toepassing	2
Gedeeltelijk	8

Toelichting

In principe zijn de verwerkingen van persoonsgegevens waar onze organisatie verwerkingsverantwoordelijk of medeverantwoordelijk voor is, in het register van verwerkingsactiviteiten opgenomen. In de zomer 2019 zijn deze verwerkingen getoetst op volledigheid en actualiteit. Geconcludeerd is dat deze toets niet naar behoren uitgevoerd kon worden omdat de organisatie niet inzichtelijk heeft welke werkprocessen zij in huis heeft. In 2020 was dit ook het geval.

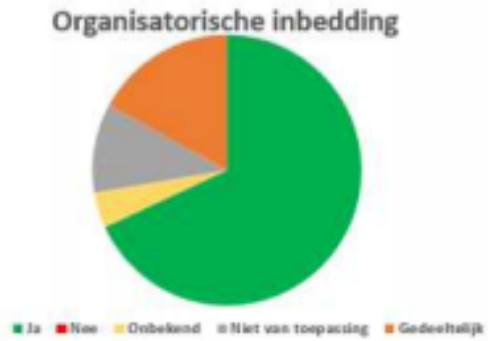
Als de gegevensverwerking een hoog privacyrisico oplevert voor de betrokken, dan wordt een DPIA uitgevoerd. Niet in alle werkprocessen is aandacht besteed aan wat gegevensbescherming en de privacywetgeving concreet betekenen voor de betreffende organisatieonderdeel en hoe

[59] Bron van de diagrammen en de bijbehorende toelichting is de jaarrapportage van de FG.

medewerkers om dienen te gaan met persoonsgegevens binnen hun taken en werkzaamheden.

Organisatorische inbedding

Resultaat	Aantal
Ja	32
Nee	0
Onbekend	2
Niet van toepassing	5
Gedeeltelijk	8



Toelichting

Om de AVG in de organisatie te borgen heeft het college van B&W een functionaris gegevensbescherming aangesteld. Deze opereert onafhankelijk van de lijnorganisatie in het team concerncontrol samen met de CISO en de privacy officer. Binnen het team Juridische Zaken is en een privacy jurist aangetrokken. Het lijnmanagement is bekend met zijn verantwoordelijkheid voor het naleven van de AVG binnen het eigen domein maar betrekt de FG niet altijd tijdig bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens. Autorisatieschema's voor geautomatiseerde systemen zijn niet overal in de organisatie aanwezig. Actuele protocollen en procedures over de wijze van omgang met persoonsgegevens zijn niet op alle organisatieonderdelen aanwezig en het is niet bekend of medewerkers die te maken hebben met bijzondere persoonsgegevens een specifieke geheimhoudingsverklaring ondertekenen, die ziet op het verwerken van die bijzondere persoonsgegevens.

Rechten van betrokkenen

Resultaat	Aantal
Ja	29
Nee	0
Onbekend	1
Niet van toepassing	1
Gedeeltelijk	1

Toelichting

Betrokkenen worden duidelijk geïnformeerd over hun rechten en hoe zij een AVG-verzoek kunnen indienen. En de gemeente heeft de processen ingericht om de rechten van betrokkenen te faciliteren. Niet alle geautomatiseerde systemen kunnen in de uitoefening van deze rechten eenvoudig voorzien en het is niet bekend of bij de aanschaf van nieuwe systemen rekening wordt gehouden met dit criterium.

Samenwerking

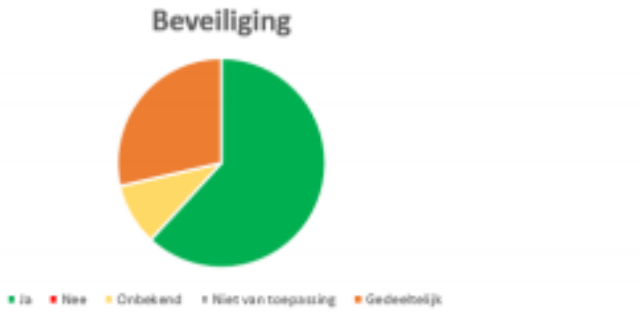
Resultaat	Aantal
Ja	16
Nee	0
Onbekend	1
Niet van toepassing	0
Gedeeltelijk	2

Toelichting

Afspraken over verwerkingen van persoonsgegevens die ontstaan binnen samenwerkingsvormen, uitbesteding van taken aan andere overheden, ketenpartners of private organisaties, worden vastgelegd in diverse juridische documenten zoals verwerkersovereenkomsten, convenanten en overeenkomsten van zorgvuldige verwerking. Het is niet bekend of al deze overeenkomsten inzichtelijk zijn. Een systematische registratie van de verwerkersovereenkomsten en de overeenkomst van opdracht verdient meer aandacht.

Beveiliging

Resultaat	Aantal
Ja	13
Nee	0
Onbekend	2
Niet van toepassing	0
Gedeeltelijk	6



Toelichting

Gemeente Rijswijk heeft een proces en een procedure voor het omgaan met incidenten in verband met persoonsgegevens (datalekken).

Toegang tot informatiesystemen is in principe beperkt tot bevoegde medewerkers door middel van autorisaties. De autorisatieschema's zijn niet altijd vastgesteld en het is niet bekend of de autorisatie regelmatig gecontroleerd worden.

Bij de inrichting van nieuwe systemen wordt niet altijd rekening gehouden met de beginselen van Privacy by Design en Privacy by Default (dataminimalisatie en privacy-vriendelijke instellingen als standaard).

Er is geen algemeen loggingbeleid en niet alle geautomatiseerde systemen zijn voorzien van logging. Dit is geen standaard functionaliteit en voor de realisatie hiervan zijn wij afhankelijk van het ontwikkeltempo van de leveranciers. Dit aandachtspunt wordt bij de implementatie van de BIO opgepakt.

Verantwoording

Resultaat	Aantal
Ja	15
Nee	1
Onbekend	3
Niet van toepassing	1
Gedeeltelijk	1

Toelichting

De verwerkingen van persoonsgegevens zijn vastgelegd in het register van verwerkingsactiviteiten. Het register kan ter beschikking gesteld worden aan de AP.

De organisatie is transparant over de verwerking van persoonsgegevens door het publiceren van privacybeleid en bijvoorbeeld het verstrekken van informatie op formulieren bij aanvragen van producten en diensten. Voorafgaand aan de verwerking van persoonsgegevens worden betrokkenen zoveel mogelijk geïnformeerd. Vanaf 2020 wordt het college geïnformeerd over de naleving van de AVG via dit verslag.

Het is niet bekend of de organisatie, wanneer de verwerking plaatsvindt op grond van toestemming van de betrokkene, kan aantonen dat de betrokkene een volwaardige toestemming heeft gegeven voor de verwerking.

Bijlage 3. Privacy volwassenheidsniveaus

1	Ad hoc	● Geen of onduidelijke privacyrollen en -verantwoordelijkheden ● Geen of nauwelijks beheersmaatregelen aanwezig ● Reactief en sturing n.a.v. incidenten ● Grote afhankelijkheid van één of enkele privacyfunctionarissen ● Onbewust onbekwaam
2	Herhaalbaar	● Privacyrollen en -verantwoordelijkheden toegewezen ● Beheersmaatregelen zijn aanwezig, maar worden op informele wijze uitgevoerd ● Standaarden en formats aanwezig: juist en in duidelijke taal ● Bewust onbekwaam
3	Bepaald	● (Privacy)medewerkers tonen eigenaarschap, d.w.z. dat de rollen en verantwoordelijkheden actief worden opgepakt ● Beheersmaatregelen worden consistent en gestructureerd uitgevoerd en zijn gedocumenteerd ● Er wordt aantoonbaar aan verplichtingen voldaan ● Verwerkingsverantwoordelijke bestuursorganen nemen beslissingen mede op grond van risicoanalyses zoals een DPIA. ● Er is een duidelijke samenhang met informatiebeveiliging ● Bewust bekwaam
4	Beheerst	● De effectiviteit van beheersmaatregelen wordt periodiek geëvalueerd in een PDCA-cyclus ● Er wordt proactief geïnformeerd door de proceseigenaar over de realisering van de geconstateerde benodigde verbeteringen in een PDCA-cyclus ● In een jaarlijkse evaluatie blijkt een correcte PDCA-cyclus ● Bewust bekwaam
5	Geoptimaliseerd	● Toekomstgericht ● Proactieve houding van het college en het bestuur ● Het verantwoordelijk management verzoekt aan de FG om hun verantwoording van een oordeel te voorzien. ● Privacy wordt gezien als een vanzelfsprekendheid ● Er wordt continue gezocht naar verbetering, zoals in de vorm van (interne of externe) tooling ● Privacy wordt gezien als een kans of unique selling point (USP) ● Er wordt verbinding gezocht met andere concerndisciplines ● Kennis en ervaringen worden actief gedeeld met gemeenten en andere relevante organisaties waardoor best practices in gemeenteland ontstaan ● Onbewust bekwaam

‘’De volgende overwegingen zijn van belang bij deze privacyvolwassenheidsniveaus:

- De proceseigenaren zijn verantwoordelijk voor de uitvoering van de controls en maatregelen en het niveau kan worden bepaald door het management. Het college of een door hen gemandateerde kan het niveau vaststellen.

- Niveau 3 wordt beschouwd als het minimumniveau dat bereikt zou moeten worden. Hiermee is niet gezegd dat de gemeente volledig compliant aan de AVG als bij alle controls niveau 3 is bereikt, omdat de maatregelen bij een control niet uitputtend zijn.
- Niveau 5 is het hoogst haalbare streefniveau. Sommige zaken spelen ook pas een rol als de basis goed op orde is, zoals het gebruik van tooling ter ondersteuning van bepaalde processen. Verder kunnen onderdelen van dit niveau dienen ter inspiratie in de vorige niveaus.
- Denk bij andere concerndisciplines (niveau 5) bijvoorbeeld aan informatiebeveiliging, informatiebeheer en risicomanagement.
- De maatregelen of delen van volwassenheidsniveaus kunnen een rol spelen bij een andere lagere niveaus. Zo wordt in niveau 5 een proactieve houding van het college en bestuur gevraagd. Het is natuurlijk mogelijk dat één of beide organen al een proactieve houding hebben, terwijl de gemeente 'slechts' bij niveau 2 is''.[60]

[60] Informatiebeveiligingsdienst en VNG, Handreiking AVG Borgingsproduct 2.0, 8 maart 2021.