Rekenkamerrapport

Informatieveiligheid en privacy in het sociaal domein

Gemeente Rijssen-Holten

Rekenkamer West Twente

Colofon:

Datum:

21 juni 2023

Opdrachtgever:

Rekenkamer West Twente

Onderzoekers:

Christan Schut

christan@necker.nl

Nick Woudstra

nick@necker.nl

Inhoudsopgave

Bestuurlijke nota

Onderzoeksverantwoording

Aanleiding

De afgelopen jaren is er veel gebeurd op het gebied van privacy- en informatieveiligheid. Zoals de invoering van de Algemene verordening gegevensbescherming (AVG) in 2018 en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG). Deze hebben de gemeente onder andere verplicht een functionaris gegevensbescherming aan te stellen. Daarnaast is de Baseline Informatiebeveiliging Overheid (BIO) ingevoerd, het basisnormenkader dat gehanteerd wordt voor informatiebeveiliging binnen alle overheidslagen.

In 2017 heeft de rekenkamer West Twente onderzoek gedaan naar de mate waarin de gemeente Rijssen-Holten de privacy van inwoners en informatieveiligheid in het sociaal domein had gewaarborgd. Aanleiding voor dat onderzoek was de aankomende invoering van de AVG. Uit het onderzoek zijn verschillende aanbevelingen voortgekomen. De invoering van de AVG is inmiddels alweer een aantal jaren geleden.

Het is belangrijk actuele standaarden rondom privacy en informatieveiligheid te waarborgen. Daarom is het van belang om opnieuw onderzoek te doen naar het onderwerp en te onderzoeken of de aanbevelingen in de praktijk zijn gebracht, of deze nog actueel zijn en of de privacy en informatieveiligheid in het sociaal domein voldoen aan de gelden wet- en regelgeving.

Tijdens de shortlistbespreking op 20 juni 2022 heeft het Presidium van de gemeente Rijssen-Holten zijn voorkeur uitgesproken voor een onderzoek naar privacy en informatieveiligheid in het sociaal domein. Het rekenkameronderzoek naar dit onderzoek moet ingaan op de betekenis van het dilemma *privacy vs. 'hulpvragen'*.

Doelstelling

Met dit onderzoek beoogt de Rekenkamer West-Twente de raad te kunnen informeren over in hoeverre de aanbevelingen uit het rapport uit 2017 nog relevant zijn, en op welke manier deze de afgelopen jaren zijn opgevolgd.

Daarnaast wil de rekenkamer meer betekenis geven aan het dilemma 'privacy versus hulpvraag': hoe wordt omgegaan met het de privacy van een hulpvrager en tegelijk goede en efficiënte hulpverlening geboden? Daarnaast is het doel te onderzoeken of de wetgeving zich sinds het onderzoek in 2017 heeft ontwikkeld. De aanbevelingen uit het eerdere onderzoek worden in lijn met eventuele nieuwe wetgeving gebracht.

De concrete doelstellingen van dit onderzoek zijn dan ook:

- De raad inzicht te bieden in de omgang met het dilemma 'privacy' vs. 'hulpvragen'.
- De raad inzicht bieden in de mate waarin aanbevelingen naar aanleiding van het onderzoek in 2017 zijn doorgevoerd.
- De raad handvatten te bieden om de privacy van inwoners en de informatieveiligheid in het sociaal domein per 2023 te waarborgen.

Vraagstelling

Uit het bovenstaande volgt de volgende hoofdvraag:

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

De hierboven geformuleerde onderzoeksvraag zullen wij beantwoorden door antwoord te geven op 9 deelvragen. De deelvragen zijn mede gebaseerd op de aanbevelingen uit het rekenkamerrapport uit 2017.

Beleid:

1. Wat is het gemeentelijk beleid en welke beleidsdoelstellingen zijn er omtrent privacy en informatieveiligheid binnen het sociaal domein?

Uitvoering:

2. Biedt het privacybeleid afdoende sturing aan medewerkers in de praktijk?
3. Wordt periodiek de stand van informatieveiligheid gemonitord?
    a. Hoe wordt er uitvoering gegeven aan monitoring met betrekking tot informatieveiligheid?
4. Zijn er afspraken gemaakt met externe ketenpartners over:
    a. de wijze waarop zij blijvende aandacht besteden aan bewustwording onder hun medewerkers?
    b. het toezicht op en verantwoording over privacy en de informatieveiligheid?
5. In welke mate en op welke manier zijn de aanbevelingen uit het onderzoek ‘Privacy en informatieveiligheid in het sociaal domein’ de afgelopen vijf jaar uitgevoerd?

Rolneming gemeenteraad:

6. Hoe wordt de raad geïnformeerd over het bereiken van doelstellingen met betrekking tot privacy en informatieveiligheid binnen het sociaal domein?
7. Wat is de kwaliteit van de informatievoorziening die de raad ontvangt?

Vooruitkijken:

8. In hoeverre zijn de aanbevelingen uit het onderzoek ‘Privacy en informatieveiligheid in het sociaal domein’ nog in lijn met de huidige wet- en regelgeving?
9. Hoe is de wetgeving sinds de uitvoering van het vorige onderzoek ontwikkeld en wat betekent dat voor de toekomst?

Onderzoeksuitvoering

Om bovenstaande vragen te kunnen beantwoorden, zijn verschillende werkzaamheden uitgevoerd. Om inzicht te krijgen in de kaders voor privacy en gegevensbescherming in het sociaal domein is als eerste

een documentanalyse uitgevoerd en heeft een oriënterend gesprek met betrokken medewerkers en de portefeuillehouder plaatsgevonden. Op basis hiervan is de documentenanalyse aangevuld met beelden vanuit de praktijk. Vervolgens zijn er gesprekken gevoerd met medewerkers en leidinggevenden in het sociaal domein. Dit heeft de praktijkkennis over de uitvoering van kaders opgeleverd. Aan de hand van een juridische analyse is er gekeken welke wetsvoorstellen in het vooruitzicht liggen en wat de impact kan zijn voor de gemeente.

De onderzoekwerkzaamheden hebben plaatsgevonden in de periode november 2022 tot april 2023. Dit is langer dan de rekenkamer had verwacht. Er is vertraging opgetreden bij het inplannen van gesprekken met medewerkers van het sociaal domein. De opgegeven contactpersoon bleek niet meer op de functie werkzaam te zijn. Na contact met de gemeentesecretaris is dit opgelost. Op 4 mei 2023 is de conceptrapportage voorgelegd aan de organisatie voor ambtelijk wederhoor. Op 2 juni 2023 is de rapportage aangeboden voor bestuurlijk wederhoor. Op 21 juni 2023 is de rapportage - nog zonder bestuurlijke reactie - aangeboden aan de gemeenteraad.

Leeswijzer

De Nota van Bevindingen bestaat uit drie hoofdstukken. In hoofdstuk 1 worden de kaders en algemene beleidsstukken ten aanzien van gegevensbescherming en privacy uiteengezet. In hoofdstuk 2 volgt de uitvoering van het beleid in de praktijk. In hoofdstuk 3 wordt ingegaan op de rol van de raad bij privacy en informatiebescherming en in hoofdstuk 4 wordt kort vooruitgekeken naar toekomstige wetswijzigingen.

Conclusies en aanbevelingen

Conclusies

Hieronder zijn de conclusies op basis van de nota van bevindingen. De conclusies zijn geordend aan de hand van de deelvragen.

Beleid

1) De gemeente Rijssen-Holten heeft actueel beleid op het gebied van informatieveiligheid. Het beleid over privacy in het sociaal domein is niet (zoals gepland) in 2022 geëvalueerd en geactualiseerd en dus verouderd. Het beleid is vertaald naar praktische handvatten voor medewerkers.

Uitvoering

2) De stand van informatieveiligheid wordt periodiek gemonitord. De gemeente voert zelfevaluaties uit en laat externe toetsen uitvoeren. Deze toetsen zijn van goede kwaliteit.
3) Er vindt interne toetsing en monitoring op privacy plaats in de teams van het sociaal domein. Deze 'intercollegiale toetsingen' zijn niet willekeurig en worden niet consequent in alle teams uitgevoerd. Dit heeft als risico dat de toetsingen een te positief beeld geven van de werkelijkheid.
4) De gemeente is verantwoordelijk voor de verwerking van persoonsgegevens, ook al wordt dit door derden gedaan (externe ketenpartners). De gemeente legt afspraken over toezicht en verantwoording met ketenpartners vast in verwerkersovereenkomsten. De afspraken worden niet gemonitord. Als er geen sprake is van een verwerkersovereenkomst worden er geen aanvullende afspraken vastgelegd. Over de daadwerkelijke naleving van afspraken over privacy door ketenpartners bestaat dus onzekerheid.
5) Van de vijf aanbevelingen uit het rekenkamerrapport 'privacy en informatieveiligheid in het sociaal domein' uit 2017 zijn er twee geheel en drie deels uitgevoerd.
6) Rijssen-Holten kenmerkt zich door een collegiale, informele cultuur. Dit zorgt ervoor dat medewerkers elkaar weten te vinden. Er wordt een afweging gemaakt tussen het strak volgen van regels en praktisch samenwerken.

Rolneming gemeenteraad

7) De gemeenteraad wordt via de P&C-cyclus geïnformeerd over gegevensbescherming en informatiebeveiliging.

Vooruitkijken

8) De werkwijze van de gemeente is in lijn met nieuwe wetsontwikkelingen die op korte termijn actief worden.

Aanbevelingen

1) **Evalueer (en actualiseer) het privacy-beleid;**

Het huidige beleid omtrent privacy is aan evaluatie (en mogelijk actualisatie) toe. In de Rapportage Gegevensbescherming en Informatiebeveiliging 2021 schrijft de gemeente dat het nodig is om het privacybeleid uit 2016 in 2022 te evalueren en een geactualiseerde versie te publiceren. Dit is nog niet gedaan. De rekenkamer beveelt aan dit alsnog te doen.

2) **Zorg voor willekeurige (intercollegiale) toetsing in de teams in het sociaal domein. Neem dit op in het kwaliteitsplan;**

Op afdelingen zijn medewerkers aangewezen die rapportages van de andere consulenten en hulpverleners toetsen. In zowel de teams jeugd als WMO dragen medewerkers zelf dossiers aan voor toetsing. Dit haalt het idee van willekeurige toetsing onderuit. De rekenkamer adviseert een systeem in te richten, dat past bij de cultuur van Rijssen-Holten, met willekeurige toetsing van dossiers. Om deze werkwijze te borgen is het aan te raden dit op te nemen in het kwaliteitsplan.

3) **Maak afspraken met externe ketenpartners over:**
    a. **de wijze waarop zij blijvende aandacht besteden aan bewustwording onder hun medewerkers;**
    b. **de toezicht op en verantwoording over privacy en de informatieveiligheid.**

De aanbeveling uit 2017 om afspraken te maken met ketenpartners over de omgang met privacy en informatieveiligheid en instellingen om een verantwoording te vragen over de manier waarop zij een juiste omgang met persoonsgegevens waarborgen én bewustwording onder hun medewerkers bevorderen, is in de afgelopen jaren beperkt uitgevoerd. De rekenkamer herhaalt daarom de aanbevelingen om hier serieus mee aan de slag te gaan.

Reactie van college van B&W

De reactie van het college van B&W volgt later.

Nota van Bevindingen

1. Kaders voor gegevensbescherming

Dit eerste hoofdstuk richt zich op het in kaart brengen van het gemeentelijk beleid op het gebied van privacy en informatieveiligheid binnen het sociaal domein. Daarbij is er in dit hoofdstuk aandacht voor het belangrijkste wettelijke kader voor gegevensbescherming, de Algemene Verordening Gegevensbescherming (hierna: AVG). Vervolgens richt dit hoofdstuk zich op de uitgangspunten in het door de gemeente vastgestelde privacybeleid en informatieveiligheidsbeleid. De focus ligt daarbij op de betekenis van deze uitgangspunten voor het sociaal domein. Daarmee geeft dit hoofdstuk antwoord op de volgende deelvraag:

1. Wat is het gemeentelijk beleid en welke beleidsdoelstellingen zijn er omtrent privacy en informatieveiligheid binnen het sociaal domein?

1.1. Inleiding

Als overheden die het dichtst bij de burger staan verwerken gemeenten veel persoonsgegevens. Met de decentralisaties op het gebied van zorg, jeugdzorg en werken en inkomen in 2015 is deze verwerking van persoonsgegevens in het sociaal domein nog eens toegenomen. In het organiseren van ondersteuning, zorg en voorzieningen is er zowel intern als extern een nauwe samenwerking nodig, zeker wanneer het uitgangspunt is om een integrale werkwijze te hanteren. Daarnaast werken gemeenten in het sociaal domein vaak samen met andere gemeenten in gemeenschappelijke regelingen. De uitbreiding van de gemeentelijke taken sinds de decentralisaties en de nauwere samenwerking, maken dat er meer aandacht nodig is voor de zorgvuldige uitwisseling en beveiliging van persoonsgegevens.

Voor het organiseren van privacy en informatieveiligheid zijn de relevante wettelijke en gemeentelijke kaders van belang. Hieronder zijn de twee belangrijkste wettelijke kaders – de Algemene Verordening Gegevensbescherming en de Baseline Informatiebeveiliging Overheid – uiteengezet. Ook worden de uitgangspunten van de twee belangrijkste beleidsdocumenten – het privacybeleid en het informatiebeveiligingsbeleid – weergegeven.

1.2. Kader voor privacy: AVG

Het belangrijkste wettelijke kader voor gegevensbescherming is de Algemene Verordening Gegevensbescherming (hierna: AVG). De AVG kent verschillende verplichtingen voor de inrichting van gegevensbescherming door organisaties die persoonsgegevens verwerken en werd op 25 mei 2018 van toepassing. In Nederland zijn de regels voor gegevensbescherming naast de AVG ook vastgelegd in de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Daar waar de AVG ruimte laat aan de nationale wetgever is deze ruimte in Nederland ingevuld in de UAVG. De AVG en de UAVG vormen daarmee een vervanging van de richtlijn 95/46/EG en de Wet bescherming persoonsgegevens (Wbp).

1.2.1. De AVG op hoofdlijnen

De AVG is van toepassing op alle verwerkingen van persoonsgegevens buiten de persoonlijke kring of huishoudelijke sfeer en binnen de werkingssfeer van het Europees recht. Dat betekent dat de verwerking van persoonsgegevens moet voldoen aan alle zes basisprincipes uit artikel 5 eerste lid van de AVG:

- Persoonsgegevens moet rechtmatig, behoorlijk en transparant gebeuren.
- Persoonsgegevens mogen alleen worden verwerkt voor het doel van verzameling en de verwerking moet redelijk en proportioneel zijn voor het bereiken van het doel van verzameling.
- De verwerking moet zich beperken tot wat minimaal nodig is voor het doel van zameling van de persoonsgegevens.
- De persoonsgegevens die worden verwerkt moeten juist zijn.
- Persoonsgegevens mogen niet langer bewaard worden dan noodzakelijk.
- Er moet vertrouwelijk met persoonsgegevens worden omgegaan en er moeten gepaste maatregelen genomen worden om de vertrouwelijkheid en integriteit van de te verwerken persoonsgegevens te garanderen.

Naast de een verwerking altijd moet voldoen aan de zes basisprincipes moet ook altijd één van de zes grondslagen uit artikel 6 eerste lid AVG moet van toepassing zijn:

- De verwerking is noodzakelijk voor de uitvoering van een overeenkomst of voor het sluiten van de overeenkomst.
- De verwerking is noodzakelijk om aan een wettelijke verplichting te voldoen.
- De verwerking is noodzakelijk in een zaak van leven en dood (vitale belangen van een persoon).
- De verwerking is noodzakelijk voor de vervulling van een taak in het algemeen belang of openbaar gezag.
- De verwerking is noodzakelijk voor gerechtvaardigde belangen, zolang de belangen van de betrokken personen niet zwaarder wegen.
- De betrokkene heeft toestemming gegeven.

Buiten dat de AVG voorwaarden stelt voor de verwerking van persoonsgegevens geeft de AVG ook verschillende meer organisatorische verplichtingen voor de bescherming van persoonsgegevens. Zo zijn organisaties die persoonsgegevens verwerken onder andere verplicht tot:

- het instellen van een register van verwerkingsactiviteiten;
- het instellen van de functionaris gegevensbescherming;
- het voorafgaand aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling (DPIA) uitvoeren;
- het raadplegen van de Autoriteit Persoonsgegevens voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit;
- de toepassing van de principes van privacy door ontwerp en standaardinstellingen (‘privacy by design & default’);
- het nemen van passende beveiligingsmaatregelen met het oog op de bescherming van persoonsgegevens;
- het onder bepaalde omstandigheden melden van een datalek bij de Autoriteit Persoonsgegevens en het informeren van betrokkenen;
- het maken van afspraken tussen verwerkingsverantwoordelijke en verwerker;
- het opstellen van privacybeleid.

1.2.2. De AVG verplicht tot een privacybeleid

Bij het verwerken van persoonsgegevens is de gemeente in de meeste gevallen de verwerkingsverantwoordelijke. Op basis van artikel 5 tweede lid AVG heeft de verwerkingsverantwoordelijke een verantwoordingsplicht en moet daardoor kunnen aantonen dat de verwerking voldoet aan de privacyregels.[1] Onderdeel van deze verantwoordingsplicht is het opstellen van een privacybeleid (ook wel gegevensbeschermingsbeleid genoemd). In een privacybeleid kan de gemeente haar visie op de wijze van gegevensverwerking geven, waardoor zij hierover op een transparante wijze kan communiceren richting inwoners van wie persoonsgegevens worden verwerkt.[2]

De AVG stelt geen harde eisen aan de precieze inhoud van het privacybeleid. De Autoriteit Persoonsgegevens heeft wel geformuleerd wat er onder meer in het privacybeleid zou moeten staan, uitgaande van de principes van de AVG. Zo moet het privacybeleid bijvoorbeeld laten zien op welke manier de gemeente voldoet aan de beginselen uit artikel 5 van de AVG, moeten de rechten van betrokkenen uiteengezet worden en moet de gemeente laten zien welke maatregelen zij neemt voor de beveiliging van persoonsgegevens.[3] Daarnaast doet de autoriteit persoonsgegevens de aanbeveling om het privacybeleid een concrete vertaling van de AVG-normen te laten zijn.[4]

1.3. Privacybeleid: gemeente Rijssen-Holten

In 2016 heeft de gemeente Rijssen-Holten een privacybeleid vastgesteld. Het privacybeleid bevat uitgangspunten voor het waarborgen van privacy en geeft een werkwijze voor de omgang met persoonsgegevens. In de Rapportage Gegevensbescherming en Informatiebeveiliging 2021 schrijft de gemeente dat het nodig is om het privacybeleid uit 2016 in 2022 te evalueren en een geactualiseerde versie te publiceren. Dit is nog niet gedaan.

1.3.1. Werken volgens de AVG levert spanning op tussen integraal werken en AVG-proof werken

In de visie van de gemeente levert het werken met de AVG een spanning op tussen het voldoen aan de regels uit het gegevensbeschermingsrecht en het hanteren van een integrale werkwijze met een nauwe interne en externe samenwerking. Voor de gemeente staat een goede dienstverlening voorop maar wil tegelijkertijd goed omgaan met de persoonsgegevens van inwoners.

[1] Artikel 5 lid 2 Algemene Verordening Gegevensbescherming.
[2] Het is niet voor iedere organisatie verplicht om een privacybeleid vast te stellen. Deze verplichting moet in verhouding staan tot de verwerkingsactiviteiten van de organisatie. Hierbij moet gekeken worden naar de aard, de omvang, de context en het doel van de gegevensverwerking. In deze afweging zullen volgens de AP gemeenten vaak verplicht zijn om een privacybeleid op te stellen. Gezien de omvang van de gemeente Zoetermeer vormt het opstellen van een privacybeleid een verplichting.
[3] Autoriteit Persoonsgegevens (2022). Verantwoordingsplicht AVG: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/verantwoordingsplicht?qa=privacybeleid&scrollto=1.
[4] https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/zes-aanbevelingen-voor-een-privacybeleid.

1.3.2. De gemeente streeft naar volwassenheidniveau 4

In 2014 heeft de gemeente laten onderzoeken in welke mate de organisatie voldoet aan het gegevensbeschermingsrecht. De uitkomst daarvan was dat de gemeente zich op het laagste niveau, niveau 1 (ad hoc) bevond.[5] Het streven van de gemeente is om op niveau 4 (gemanaged) te komen. Het privacybeleid moet daar een bijdrage aan leveren.

1.3.3. Belangrijke rol voor de FG als toezichthouder

Het college is de eindverantwoordelijke voor de naleving van de AVG in de gemeente en legt daar verantwoording over af aan de gemeenteraad, stelt het privacybeleid. De functionaris gegevensbescherming (hierna: FG) heeft de verantwoordelijkheid om toezicht te houden op de organisatie en geeft daarom uitvoering aan de volgende taken:

- adviseren en informeren van het college en de organisatie op de invulling van de plichten uit de AVG;
- toezien op de naleving van privacywetgeving en het privacybeleid;
- toezien op uitvoering van de toegewezen verantwoordelijkheden;
- zorgen voor bewustwording en opleiding van personeel dat betrokken is bij de verwerking van persoonsgegevens en audits;
- adviseren over en toezien op de uitvoering van DPIA's;
- zijn van contactpunt voor de autoriteit persoonsgegevens.

1.3.4. Het privacybeleid gaat in op beginselen artikel 5 AVG en noodzaak van toestemming

Onder de titel uitgangspunten gaat het privacybeleid uitgebreid in op de beginselen voor de verwerking van persoonsgegevens uit artikel 5 van de AVG, zoals doelbinding (De gegevens mogen vervolgens in principe alleen voor het vastgelegde doel worden verwerkt), dataminimalisatie en de opslagbeperking. Alle beginselen worden voorzien een uitleg.

Naast de beginselen uit artikel 5 van de AVG gaat het privacybeleid in op wanneer het nodig is om toestemming te vragen aan een betrokkene.

1.3.5. Het privacybeleid vormt een kader voor interne en externe uitwisseling van persoonsgegevens

Het privacybeleid bevat ook een afwegingskader voor het delen van informatie binnen de gemeente. De gemeente wil graag integraal werken. Dat betekent dat gegevens die zijn verzameld voor een bepaald doel soms worden verwerkt voor een ander doel. Als daar geen expliciete toestemming voor is gegeven, dan kijkt de gemeente naar vijf punten:

- het verband tussen de twee doeleinden;
- het kader waarin de persoonsgegevens zijn verzameld en de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke;
- de aard van de persoonsgegevens;
- de mogelijke gevolgen voor de betrokkene;
- het bestaan van passende waarborgen, waaronder eventueel versleuteling of pseudonimisering.

[5] Het Handreiking-AVG-borgingsproduct van de Informatie Beveiligingsdienst bevat een volwassenheidsmodel dat aansluit bij het Privacy Maturity Model van de International Association of Privacy Professionals. Hierin zijn vijf volwassenheidsniveau geformuleerd waarin organisaties zich kunnen bevinden.

Voor de uitwisseling van gegevens met externe partijen maakt de gemeente afspraken over de uitwisseling en over de vertrouwelijkheid daarvan. Met verwerkers sluit de gemeente verwerkersovereenkomsten.

Tot slot zijn ook de rechten van betrokkenen uit het derde hoofdstuk van de AVG opgenomen in het privacybeleid. Zo zijn bijvoorbeeld het recht op inzage en het recht op correctie opgenomen.

1.4. Kader voor informatiebeveiliging: BIO

Naast de bepalingen uit de AVG en de UAVG is de Baseline Informatiebeveiliging Overheid (hierna: BIO) van belang als het gaat om gegevensbescherming. De BIO[6] vormt als baseline voor overheden een belangrijk kader voor informatiebeveiliging. De BIO is sinds 1 januari 2020 van kracht en zorgt voor één normenkader voor informatiebeveiliging voor gemeenten, waterschappen, provincies en het Rijk. De BIO is de opvolger van de Baseline Informatiebeveiliging Gemeenten (BIG), met in vergelijking minder maatregelen, het toewijzen van maatregelen aan eindverantwoordelijken en meer nadruk op risicomanagement.[7]

1.4.1. De BIO in het kort

De BIO vormt voor gemeenten zowel een richtlijn als een hulpmiddel om informatiebeveiliging te organiseren. Om te werken volgens de BIO is het voor de gemeente van belang om in kaart te brengen welke beveiligingsmaatregelen er zijn binnen de gemeente, wat de belangrijkste processen zijn en wie eigenaar is van die processen. Vervolgens moet het basisbeveiligingsniveau van die processen worden bepaalt door middel van een zogenaamde Business Impact Analyse (BIA). Binnen de BIO wordt onderscheid gemaakt tussen drie basisbeveiligingsniveaus: BBN1, BBN2 en BBN3. De inzet van controlemaatregelen en de verdeling van verantwoordelijkheden binnen de organisatie is afhankelijk van het basisbeveiligingsniveau.

Voor gemeenten is BBN2 het uitgangspunt. BBN2 is van toepassing wanneer het gaat om informatie die vertrouwelijk is, informatie waarbij incidenten leiden tot bestuurlijke commotie of informatie die van belang is voor de veiligheid van andere informatiesystemen.[8] Wanneer BBN2 te zwaar is dan is BBN1 van toepassing en wanneer BBN2 niet zwaar genoeg is dan is BBN3 van toepassing.[9]

1.4.2. Het informatiebeveiligingsbeleid en informatiebeveiligingsplan

Om informatiebeveiliging vorm te geven in de gemeente is het van belang om een informatiebeveiligingsbeleid op te stellen. Dit beleidsdocument beschrijft de gemeentelijke uitgangspunten op het gebied van informatieveiligheid. De BIO stelt dat in ieder geval de volgende zaken in het informatiebeveiligingsbeleid moeten staan:[10]

[6] Term opgenomen in de begrippenlijst
[7] Informatiebeveiligingsdienst (2022). Baseline Informatiebeveiliging Overheid: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/.
[8] Baseline Informatiebeveiliging Gemeenten (2020), p.14.
[9] Baseline Informatiebeveiliging Gemeenten (2020), p.21.
[10] Baseline Informatiebeveiliging Gemeenten (2020), p.22.

- De strategische uitgangspunten en randvoorwaarden voor informatiebeveiliging dienen te worden vastgelegd. Daarbij is in het bijzonder de inbedding en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid van belang;
- De verantwoordelijkheidsverdeling op het gebied van informatiebeveiliging;
- De toewijzing van verantwoordelijkheden voor ketens van informatiesystemen;
- De gemeenschappelijke betrouwbaarheidseisen en normen van de organisatie
- De frequentie waarmee informatiebeveiligingsbeleid periodiek moet worden geëvalueerd;
- De wijze van bevordering van beveiligingsbewustzijn.

Om het informatiebeveiligingsbeleid te vertalen naar de praktijk moeten gemeenten periodiek een informatiebeveiligingsplan opstellen. Het informatiebeveiligingsplan is een projectplan met aandachtspunten op het gebied van informatiebeveiliging om te zorgen voor de implementatie van de ontbrekende beveiligingsmaatregelen.[11] Dit informatiebeveiligingsplan kan worden opgesteld als één document voor alle processen of bestaan uit meerdere systeem-specifieke plannen.

1.5. Informatiebeveiligingsbeleid: gemeente Rijssen-Holten

Het college van de gemeente Rijssen-Holten heeft in 2019 het informatiebeveiligingsbeleid 2020 vastgesteld. Dit beleid vormt een vervanging van het informatiebeveiligingsbeleid 2017-2020 en wordt op tactisch niveau aangevuld met specifieke beleidsdocumenten per onderwerp.

De concrete beveiligingsmaatregelen voor informatiebeveiliging, zo stelt het informatiebeveiligingsbeleid, zijn opgenomen in het jaarlijks door de directie op te stellen informatiebeveiligingsplan.[12] Tijdens dit onderzoek zijn dergelijke informatiebeveiligingsplannen niet aangetroffen.

1.5.1. Belangrijkste doelen en uitgangspunten

Het informatiebeveiligingsbeleid kent verschillende strategische doelen en uitgangspunten. De belangrijkste daarvan zullen hier beknopt worden weergegeven.

De belangrijkste strategische doelen zijn:[13]

- Het managen van de informatiebeveiliging.
- Het minimaliseren van risico's van menselijk gedrag.
- Het voorkomen van ongeautoriseerde toegang.
- Het garanderen van correcte en veilige informatievoorzieningen.
- Het beheersen van de toegang tot informatiesystemen.
- Het waarborgen van veilige informatiesystemen.
- Het adequaat reageren op incidenten.
- Het beschermen en correct verwerken van persoonsgegevens van burgers en medewerkers.

De belangrijkste uitgangspunten zijn:[14]

[11] Handreiking BIO voor kleine gemeenten (2019), p.14.
[12] Informatiebeveiligingsbeleid 2020, p.8.
[13] Informatiebeveiligingsbeleid 2020, p.8.
[14] Informatiebeveiligingsbeleid 2020, p.8/9.

- De uitvoering van informatiebeveiliging is een verantwoordelijkheid van de teammanagers. Alle informatiebronnen en -systemen in de gemeente hebben een interne eigenaar die de vertrouwelijkheid en/of waarde bepaald van de informatie. De primaire verantwoordelijkheid voor de bescherming van informatie ligt bij de eigenaar van de informatie.
- Door periodieke controle, organisatie brede planning en coördinatie wordt de kwaliteit van de informatievoorziening verankerd binnen de organisatie. Het informatiebeveiligingsbeleid en het (in de praktijk niet aanwezige) informatiebeveiligingsplan vormen het fundament voor een betrouwbare informatievoorziening. In het informatiebeveiligingsplan dient de betrouwbaarheid van de informatievoorziening organisatiebreed te worden benaderd. Het plan zou periodiek moeten worden bijgesteld op basis van nieuwe ontwikkelingen, registraties in het incidentenregister en bestaande risicoanalyses.
- Informatiebeveiliging is een continu verbeterproces. 'Plan Do Check Act' vormt het managementsysteem van informatiebeveiliging.
- De gemeente stelt de benodigde mensen en middelen beschikbaar voor informatieveiligheid.
- Regels en verantwoordelijkheden voor het beveiligingsbeleid dienen te worden vastgelegd en vastgesteld.
- Iedere medewerker, zowel vast als tijdelijk, intern of extern, is verplicht waar nodig gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht en bij vermeende inbreuken hiervan melding te maken.

1.5.2. Verdeling van verantwoordelijkheden

De verantwoordelijkheid voor een zorgvuldige informatiebeveiliging ligt bij het college. Het college stelt het informatiebeveiligingsbeleid vast en is verantwoordelijk voor het ontwikkelen, beoordelen en evalueren van het beleid. De directie is vervolgens verantwoordelijk voor de uitvoering van het beleid en de sturing binnen de organisatie. De directie dient jaarlijks een informatiebeveiligingsplan vast te stellen, ervoor te zorgen dat informatiesystemen altijd onder een specifieke teammanager vallen en erop toe te zien dat teammanagers adequate maatregelen nemen voor de bescherming van informatie. De teammanagers zijn verantwoordelijk voor de informatie onder hun verantwoordelijkheid en leveren input voor het wijzigen of opnemen van maatregelen of procedures. Daarnaast dragen zij het beveiligingsbeleid uit in hun team, signaleren de belangrijkste bedreigingen en evalueren beveiligingsincidenten.[15]

1.5.3. Verantwoording

Het college is eindverantwoordelijk voor informatiebeveiliging. De verantwoording voor het gevoerde beleid verloopt via de Jaarrapportage gegevensbescherming en informatiebeveiliging. Onderdeel van de verantwoording is de ENSIA-systematiek[16]. De informatiebeveiligingsfunctionaris (IBF) is aangewezen als ENSIA-coördinator en maakt ENSIA-rapportages op basis van de input van de teammanager.[17] De jaarrapportage bevat ook de collegeverklaring waarin het college aangeeft in hoeverre de gemeente volgens de ENSIA-verantwoording voldoet aan de BIO-normering.[18]

[15] Informatiebeveiligingsbeleid 2020, p.10.
[16] Term opgenomen in begrippenlijst.
[17] Informatiebeveiligingsbeleid 2020, p.10.
[18] Informatiebeveiligingsbeleid 2020, p.11.

1.6. Privacy in het sociaal domein

Waar de AVG en BIO het algemene kader vormen voor privacy en informatiebeveiliging, zijn er voor het sociaal domein, naast de Algemene Wet Bestuursrecht, specifiek vier wetten relevant: de Jeugdwet, de Wet maatschappelijke ondersteuning (Wmo), de Participatiewet en de Wet gemeentelijke schuldhulpverlening (Wgs). Deze wetten geven de gemeente verschillende taken binnen het sociaal domein, zoals schuldhulpverlening en jeugdhulp. Andere wetten die zijdelings van belang zijn binnen dit domein, zijn de Wet passend onderwijs, Wet langdurige zorg en de Wet publieke gezondheid. De Jeugdwet, Wmo, Participatiewet en Wgs geven de gemeente, naast taken, ook grondslagen voor het verwerken van persoonsgegevens zodat gemeenten de beschreven taken uit kunnen voeren. Dit zijn:

- Hoofdstuk 5 van de Wet maatschappelijke ondersteuning (Wmo) 2015;
- Hoofdstuk 7 van de Jeugdwet;
- Paragraaf 6.6 van de Participatiewet;
- Artikel 8 van de Wet gemeentelijke schuldhulpverlening.

1.6.1. Wmo

De Wmo geeft het college onder voorwaarden een grondslag voor de verwerking van persoonsgegevens zolang die verwerking noodzakelijk is "*voor de beoordeling van diens behoefte aan ondersteuning van zijn participatie of zelfredzaamheid dan wel opvang of beschermd wonen*" en is het college onder voorwaarden bevoegd tot de verwerking van persoonsgegevens van de mantelzorger of andere personen in het sociale netwerk van een cliënt om "*vast te stellen welke hulp deze aan de cliënt biedt of kan bieden*".[19] Daarnaast geeft de Wmo het college een grondslag voor de verwerking van persoonsgegevens van cliënten die noodzakelijk zijn voor de uitvoering van een overeenkomst met een aanbieder van maatwerkvoorzieningen.[20]

In de Wmo is tevens (onder hoofdstuk 4, artikel 5.1.6) de grondslag opgenomen voor de verwerking van gegevens door Veilig Thuis. Dit betreft casussen over huiselijk geweld, kindermishandeling en onveilige situaties.

Het kan voorkomen dat tijdens het onderzoek naar de situatie en de zorg- en ondersteuningsbehoefte van de cliënt gegevens moeten worden opgevraagd bij een zorgverlener met een medisch beroepsgeheim, zoals de huisarts. De zorgverlener zal de afweging maken wat hij wel en niet kan verstrekken en uitdrukkelijke toestemming nodig hebben van zijn patiënt om deze gegevens te kunnen uitwisselen met de gemeente. Hier is een gestandaardiseerd toestemmingsformulier voor opgesteld door de gemeente voor zowel cliënt als medisch professional. Deze toestemming dient vervolgens ook opgenomen te worden in het dossier van de inwoner.

1.6.2. Jeugdwet

De jeugdwet geeft het college een grondslag voor de verwerking van persoonsgegevens voor[21]:

- de toeleiding naar jeugdhulp;
- voor het doen van een verzoek tot onderzoek bij de raad voor de kinderbescherming of de uitvoering van kinderbeschermingsmaatregelen of jeugdreclassering;

[19] Artikel 5.1.1. Wet Maatschappelijke Ondersteuning.
[20] Artikel 5.1.1. Wet Maatschappelijke Ondersteuning.
[21] Artikel 7.4.0. Jeugdwet

- de bekostiging van preventie, jeugdhulp, kinderbeschermingsmaatregelen, jeugdreclassering of werkzaamheden als bedoeld in de artikelen 6.1.2, vijfde lid, 6.1.3, derde lid, en 6.1.4, derde lid;
- het verrichten van controle of fraude-onderzoek.

Een beperkt juridisch kader voor interne als externe gegevensdeling

In de jeugdhulp spelen twee aspecten van privacy een rol: de borging van privacy binnen organisaties (waaronder gemeenten) en de uitwisseling van gegevens tussen organisaties. De wet maakt daarnaast onderscheid tussen toeleiding (gemeentelijke taak) en de uitvoering van jeugdhulp (professionals)

Intern

Als de gemeente persoonsgegevens verwerkt heeft zij daar niet altijd toestemming voor nodig. Wanneer de verwerking van persoonsgegevens, waaronder bijzondere persoonsgegevens, strikt noodzakelijk is voor de uitoefening van sociale zekerheids- en sociale beschermingsrechten dan biedt artikel 7.4 van de jeugdwet daar grondslag voor (in het kader van toeleiding). Proportionaliteit en subsidiariteit zijn hierin wel van belang; De hulpvraag van de cliënt is leidend bij het verwerken van persoonsgegevens. De ambtenaar registreert uitsluitend die persoonsgegevens die noodzakelijk zijn voor de hulpvraag en de toeleiding naar zorg naar aanleiding van die hulpvraag.

Of informatie van een cliënt binnen de gemeente (bijvoorbeeld met ambtenaren van andere afdelingen) gedeeld mag worden verschilt. Bij domein-overstijgende overleggen is vrijwel altijd toestemming nodig van de cliënt (tenzij er sprake is van de mogelijkheid om ernstig nadeel voor betrokkenen te voorkomen). Indien het mogelijk is om een casus anoniem te bespreken, dan is dit ook verplicht.

Extern

Er bestaat momenteel geen adequaat juridisch kader voor de samenwerking tussen verschillende hulpverleners, onderwijsinstanties, organisaties in het voorveld en overheden. In dit verband wordt toestemming als de meest gangbare juridische basis beschouwd. De toestemming van kinderen en hun ouders is echter onderhevig aan diverse voorwaarden die de professional dient te respecteren. Bovendien dient de professional aan te tonen dat de toestemming daadwerkelijk verleend werd. In het bijzonder bij de uitwisseling van gezondheidsgegevens tussen externe partners is het essentieel dat alle betrokken partijen op de hoogte zijn van de verleende toestemming. Voor de uitwisseling van gegevens is toestemming nodig van:

- ouders, als het kind jonger is dan 12 jaar;
- ouders en kind, als het kind tussen 12 en 16 jaar is;
- het kind, als het 16 jaar of ouder is. De ouders blijven ook in dit geval nog steeds verantwoordelijk.

.

1.6.3. De participatiewet

Voor de uitvoering van de Participatiewet zijn veel persoonsgegevens nodig. De wet gaat immers over uitkeringen en werk. Beide afgestemd op de persoonlijke situatie van de aanvrager. De gemeente moet daarvoor de persoonlijke situatie van de aanvrager in kaart brengen, en daarmee vaak ook van het gezin. Maar ook bij heronderzoeken, controles en fraudeonderzoeken worden persoonsgegevens verwerkt. De wet biedt de volgende kaders:

- *Een ieder is verplicht desgevraagd en bevoegd uit eigen beweging aan het college kosteloos opgaven en inlichtingen te verstrekken omtrent feiten en omstandigheden die noodzakelijk zijn voor de uitvoering van deze wet door het college ten opzichte van een persoon te wiens behoeve bijstand is gevraagd of wordt verleend en die in zijn dienst dan wel voor hem arbeid verricht, heeft verricht of zou kunnen gaan verrichten. De verplichting strekt zich mede uit tot de inkomsten van een persoon van wie kosten van bijstand ingevolge paragraaf 4 worden of kunnen worden teruggevorderd of op wie kosten van bijstand ingevolge paragraaf 5 worden of kunnen worden verhaald.*[22]
- *Het college is verplicht, indien het bij de uitvoering van deze wet het gegronde vermoeden krijgt van een misdrijf dat is gepleegd ten nadele van een Nederlands of buitenlands uitvoeringsorgaan van de sociale verzekeringswetten of van een Nederlands of buitenlands overheidsorgaan, voorzover dit is belast met het verrichten van uitkeringen, het doen van verstrekkingen dan wel het heffen van bijdragen, het betrokken orgaan hiervan in kennis te stellen.*[23]

1.6.4. De Wgs, ofwel Wet gemeentelijke schuldhulpverlening

De Wgs regelt dat mensen met (dreigende) problematische schulden bij gemeenten terecht kunnen voor onder meer advies, schuldbemiddeling of een saneringskrediet. De wet is gewijzigd in 2021 en heeft gemeenten daarmee meer bevoegdheden gegeven in de gegevensuitwisseling in het kader van schuldenpreventie. Sommige schuldeisers moeten betalingsachterstanden van inwoners onder voorwaarden delen met de gemeente voor vroegsignalering. Momenteel zijn dat woningverhuurders, zorgverzekeraars en drinkwater- en energiebedrijven. De gemeente is vervolgens bevoegd om contact op te nemen met de desbetreffende inwoner. Tevens mag de gemeente alle schulden, waaronder lokale belastingschulden en hypotheekachterstanden, inventariseren om een plan van aanpak op te stellen.

Om inkomen en vermogen vast te stellen, kan de gemeente de gegevens gebruiken die de gemeente zelf heeft verwerkt op grond van de Wmo, Participatiewet en Jeugdwet. Ook kan de gemeente voor dat doel gegevens opvragen bij onder meer de Belastingdienst, UWV, SVB, Kadaster, LBIO en RDW. Dit is echter pas toegestaan als de inwoner heeft ingestemd met het opstellen van een zogeheten plan van aanpak.

Het gouden ei voor een integrale sociaal domeinaanpak?

De autoriteit persoonsgegevens heeft een richtlijn opgesteld voor de uitvoering van de Wgs. Daarin is het volgende opgenomen: "*De Wgs biedt geen mogelijkheid voor domeinoverstijgende (integrale) gegevensverwerking in het sociaal domein in den brede. De Wgs bepaalt namelijk dat gegevens uit andere domeinen alleen mogen worden verwerkt als dat noodzakelijk is voor een specifiek doel, namelijk het vaststellen van een plan van aanpak voor schuldhulpverlening. De Wgs faciliteert geen verwerkingen van persoonsgegevens voor doeleinden die het domein van de Wgs overstijgen. Zoals gezinnen waarbij, naast schuldenproblematiek, ook jeugdzorg en/of de strafrechtketen is betrokken*" Daarbij komt ook dat de benadering van andere afdelingen binnen de gemeenten alleen is toegestaan vanuit de Wgs, niet andersom. Dus deze wet biedt geen kader voor integraliteit.

1.6.5. Privacyprotocol sociaal domein

Om te zorgen voor een vertaling van taken en bevoegdheden van de gemeente binnen het sociaal domein en om te zorgen voor een vertaling van het gemeentelijke beleidskader, heeft de gemeente een privacyprotocol opgesteld.[24] In dit protocol is in grote lijnen opgenomen welke gegevens op welke

[22] Artikel 63 Participatiewet
[23] Artikel 66 Participatiewet.
[24] Privacy protocol Sociaal Domein gemeente Rijssen-Holten 2018

manier worden vastgelegd, wie daar toegang toe heeft, welke protocollen er gelden voor interne en externe uitwisseling en de wijze waarop er toestemming gevraagd dient te worden.

Om te zorgen voor een vertaling van privacybeleid en het informatiebeveiligingsbeleid naar de praktijk van het sociaal domein heeft de gemeente in 2020 het Gedragsprotocol Sociaal Domein gemeente Rijssen-Holten voor intern gebruik vastgesteld. Het gedragsprotocol moet ambtenaren richtlijnen geven voor de verwerking van persoonsgegevens in het sociaal domein en moet handvatten bieden voor de borging van privacy. Het gedragsprotocol kan gelezen worden als praktische vertaling van de algemene regels in het privacyprotocol en de AVG. Hieronder worden enkele onderdelen uit het gedragsprotocol toegelicht:

Het verschil tussen reguliere en bijzondere persoonsgegevens

Persoonsgegevens zijn alle herleidbare gegevens van natuurlijk persoon zoals naam, adres, woonplaats, BSN en geboortedatum. Godsdienst/geloofsovertuiging, ras, etnische afkomst, politieke gezindheid, gezondheid, genetische gegevens, seksualiteit en lidmaatschap vakvereniging, strafrechtelijke veroordelingen/feiten zijn bijzondere persoonsgegevens.

Waar ‘gewone’ persoonsgegevens in principe mogen worden verwerkt, als dat op basis van een grondslag en zorgvuldig gebeurt, is de verwerking van ‘bijzondere persoonsgegevens’ juist verboden, behoudens strenge wettelijke uitzonderingen. Het gedragsprotocol beschrijft: *"Bijzondere persoonsgegevens mogen wel worden verwerkt wanneer dit strikt noodzakelijk is voor de ondersteuning aan de betrokkene, in het kader van vitale belangen en de uitoefening van sociale zekerheids- en sociale beschermingsrechten."*

Rechten van betrokkene uiteengezet

In het gedragsprotocol zijn ook de rechten van betrokkenen beschreven, en worden handvatten geboden om hier om zorgvuldige manier mee om te gaan. De rechten van betrokkenen zijn:

- Recht op informatie;
- Recht op kennisgeving;
- Recht op inzage en afschrift;
- Recht op rectificatie;
- Recht op verwijderen van gegevens;
- Recht op beperking van de verwerking;
- Recht op overdraagbaarheid van gegevens;
- Bezwaar en klachten.

In het kader van dit onderzoek is het in het relevant om te kijken naar het recht van informatie, het recht op verwijderen en het recht op overdraagbaarheid van gegevens.

De gemeente is verplicht de inwoner te informeren over het feit dat er gegevens van hem/haar worden verwerkt, wie de verantwoordelijke voor deze verwerking is en met welk doel de verwerking plaatsvindt. Deze informatieplicht is een uitwerking van het transparantiebeginsel dat is bedoeld om de betrokkenen in staat te stellen de verwerkingsverantwoordelijke (in rechte) aan te spreken. De leeftijdsgrenzen zoals eerder genoemd gelden ook voor het informeren van betrokkenen.

Het recht op verwijderen van gegevens komt voort uit de AVG. Al blijkt dat in het geval van zorgverlening de grenzen soms vaag zijn. Het wissen van gegevens hoeft niet als het bewaren van het dossier belangrijk(er) is voor een ander dan de betrokkene. In 2021 heeft het Hof een uitspraak gedaan over de weging van het belang van het kind in het verwijderen van informatie[25] waaruit bleek dat het belang van de ouder (om een dossier te wissen) niet opweegt tegen het belang van het kind om de veiligheid te waarborgen. Het gedragsprotocol biedt de medewerkers handvatten hoe om te gaan met een AVG-verzoek. Dit gaat altijd via de lijn teammanager – privacy officer. Medewerkers voeren nooit zelf AVG-verzoeken uit.

Als de betrokkene toestemming heeft gegeven voor het opslaan/bewerken van persoonsgegevens heeft de betrokkene het recht deze persoonsgegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt. Hiervoor kan hij een schriftelijk verzoek indienen. Voor activiteiten die voortkomen uit de wet (en daarmee wettelijk uitgevoerd worden door de gemeente waarin de inwoners woont) geldt deze bepaling uiteraard niet.

[25] https://www.hetwetshuys.nl/blog/scheiding/uitspraak-hof-privacy-in-de-jeugdhulp/

2. Uitvoering

Dit hoofdstuk gaat in op de vertaling van de wettelijke en gemeentelijke kaders naar de praktijk van gemeente. De focus ligt daarbij op het sociaal domein. Daarmee geeft dit hoofdstuk antwoord op de volgende deelvraag:

2. *Biedt het privacybeleid afdoende sturing aan medewerkers in de praktijk?*
3. *Wordt periodiek de stand van informatieveiligheid gemonitord? Hoe wordt er uitvoering gegeven aan monitoring met betrekking tot informatieveiligheid?*
4. *Zijn er afspraken gemaakt met externe ketenpartners over:*
   a. de wijze waarop zij blijvende aandacht besteden aan bewustwording onder hun medewerkers?
   b. de toezicht op en verantwoording over privacy en de informatieveiligheid?
5. *In welke mate en op welke manier zijn de aanbevelingen uit het onderzoek 'Privacy en informatieveiligheid in het sociaal domein' de afgelopen vijf jaar uitgevoerd?*
6. *In hoeverre zijn de aanbevelingen uit het onderzoek 'Privacy en informatieveiligheid in het sociaal domein' nog in lijn met de huidige wet- en regelgeving?*

2.1. Privacybeleid in de praktijk

2.1.1. Algemene bekendheid en activiteiten hieromtrent

Medewerkers vormen een cruciale schakel in het waarborgen van informatiebeveiliging en privacy. Wanneer medewerkers niet alert zijn en de voorgeschreven richtlijnen en tips niet opvolgen, kunnen er alsnog problemen ontstaan. Het is dan ook van essentieel belang dat medewerkers zich bewust zijn van mogelijke risico's en dat dit bewustzijn voortdurend wordt gestimuleerd. De gemeente besteedt op verschillende manieren aandacht aan dit onderwerp. Zo spelen de FG en de privacy officer een belangrijke rol bij het bevorderen van dit bewustzijn.

De gemeente kent een actieve omgang met het beleid en gedragsregels omtrent privacy in het sociaal domein. De gedragscode is een levend document, opgesteld om praktische handvatten te bieden (Op het informatieplatform Siep wordt actief en passief informatie gedeeld over privacy en veiligheid) en de privacy officer is in het verleden langs gekomen om het beleid en de regels toe te lichten. Uit gesprekken blijkt dat dit als prettig wordt ervaren. De dagelijkse werkdruk zorgt er echter ook voor dat de kaders vooral in de praktijk, op basis van ervaring, worden toegepast en er weinig naar het protocol wordt gegrepen. In de gesprekken is aangegeven dat het goed zou zijn om eens per jaar een bijeenkomst te hebben waarin alle kennis wordt opgefrist en het onderwerp meer ruimte krijgt in de onboarding en het inwerkprogramma.

2.1.2. Privacy in het sociaal domein

De beleidsregels, gedragscodes en documenten zijn allen online en offline beschikbaar. Toch blijkt dat in de praktijk de dilemma's niet altijd zo zwart wit zijn zoals beschreven in de gedragscode of het protocol. Hieronder worden enkele praktijkvoorbeelden genoemd over de omgang met gegevens van inwoners.

Ruimte voor registratie van bijzondere persoonsgegevens is beperkt

Bij het indienen van een aanvraag door een cliënt, het uitvoeren van een behoeftenonderzoek of triage is het doorgaans vereist om naast reguliere persoonsgegevens ook bijzondere of gevoelige gegevens van de cliënt te verkrijgen, zodat de aanvraag beoordeeld kan worden en een correct besluit genomen kan worden. Denk hierbij bijvoorbeeld aan ziektebeelden en diagnoses. Het principe hierbij is om alleen de vereiste gegevens te vragen voor de beoordeling van de aanvraag en geen overbodige informatie te verzamelen, zo schrijft de wet en het lokale beleid in Rijssen-Holten voor. In het geval van gevoelige of bijzondere persoonsgegevens is het aanbevolen om extra zorgvuldig na te gaan of er een legitieme basis is voor het opvragen van deze gegevens en of het noodzakelijk is om ze te verzamelen. Indien er geen legitieme basis is voor de verwerking van bijzondere persoonsgegevens, is het niet toegestaan om deze te verwerken.

In de praktijk betekent dit dat het noteren van bijzondere persoonsgegevens in dossiers over het algemeen niet in toegestaan en leidt tot in sommige gevallen tot enigszins omfloerste beschrijvingen van de situatie van client of betrokkene. Een goed voorbeeld is de praktijk in de Wmo. Een diagnose mag bijvoorbeeld niet worden opgenomen in het dossier. Je krijgt geen voorzieningen op basis van een aandoening maar op basis van beperkingen. Het is daarmee ook niet van belang om op te nemen.

Waar het gedragsprotocol helder is, is er toch discussie over het opnemen van diagnostiek. Uit gesprekken blijkt dat de juristen van Wmo in bepaalde gevallen van mening zijn dat het wel toegestaan is om diagnoses te noemen. Specifiek binnen jeugd kan een diagnose een belangrijk onderdeel zijn van de onderbouwing van een besluit. Dit wordt dan ook met enige regelmaat vastgesteld.

Toetsing en monitoring

In de gemeente Rijssen-Holten is het zo geregeld dat er intern onderzoek gedaan wordt naar de kwaliteit van adviezen. Voorheen was er sprake van intercollegiale toetsing, zoals opgenomen in het kwaliteitsplan. Daarnaast vinden er incidentele externe toetsingen plaats. Op afdelingen zijn medewerkers aangewezen die rapportages van de andere consulenten en hulpverleners toetsen. Dit is vak- en afdelingsgebonden in verband met de informatie in de dossiers. Onderdeel van deze intercollegiale toetsing is een toets aan het gedragsprotocol en privacybeleid, de nadruk ligt echter op inhoudelijke toetsing.

Uit gesprekken blijkt dat hier niet consequent uitvoering aan wordt gegeven. Men ziet de toetsing ook als een afrekening. Op de afdeling Wmo werd eerst gewerkt met een steekproef voor het toetsen van de rapportages. Dit gaf een te hoge drempel. Nu is de afspraak dat iedere consultent maandelijks een rapportage aanlevert ter toetsing. Daarmee toetst deze afdeling ongeveer tien procent van de rapportages. Dit beeld werd ook in andere gesprekken bevestigd. Ook op de afdeling Jeugd wordt er gewerkt met het zelf ter toetsing aandragen van dossiers. Gevolg daarvan is dat sommige medewerkers dossiers aanleveren om iets van te leren, moeilijke dossiers of dossiers met een pregnant dilemma

terwijl andere medewerkers zogenoemde 'voorbeelddossiers' aangedragen die niet bijdragen aan het lerend vermogen. De medewerker kan hierin zelf dus erg sturen.

De balans tussen bureaucratie en praktisch werken wordt opgezocht

Binnen de organisatie lopen collega's van verschillende afdelingen bij elkaars lang met vragen over klanten. Inwoners zijn hiervan impliciet op de hoogte, bijvoorbeeld omdat dit is verteld in een gesprek met de betreffende inwoner. De organisatie legt dit niet vast in een toestemmingsformulier. In 2020 heeft de VNG hierover gepubliceerd in een onderzoek genaamd 'Wijkteams en het pettenvraagstuk'.

Het pettenvraagstuk

Sinds de decentralisatie van overheidstaken zijn medewerkers in het sociaal domein vaak belast met meerdere 'petten'. Voor elke 'pet' kan een ander juridisch kader van toepassing zijn op de verwerking van persoonsgegevens.

Een voorbeeld hiervan is wanneer een moeder en kind zich melden bij een wijkteam met een hulpvraag. Een medewerker van het wijkteam verleent preventieve jeugdhulp, maar kan het kind ook via de gemeente doorverwijzen naar specialistische jeugdhulp (toeleiding). Voor de eerste taak geldt het beroepsgeheim van de jeugdhulpverlener, terwijl de tweede taak namens/door de gemeente wordt uitgevoerd en andere regels van toepassing zijn. Dit kan onduidelijkheid geven in de praktijk.

Als de gegevens onder het beroepsgeheim van de jeugdhulpverlener vallen, is er een plicht tot geheimhouding met uitzonderingsmogelijkheden. Echter, wanneer de medewerker gegevens deelt in het kader van de toeleidingstaak, geldt het wettelijk beroepsgeheim van de jeugdhulpverlener niet en mag de medewerker gegevens delen met andere partijen als dat noodzakelijk is om de toeleidingstaken goed uit te voeren. Hierbij houdt de professional altijd rekening met zijn beroepscode, maar deze kan verschillend uitpakken voor het verlenen van hulp versus het toeleiden naar hulp.

2.2. Monitoring informatieveiligheid

De jaarrapportages bevatten een weergave van de informatieveiligheid in de gemeente. Om informatieveiligheid in kaart te brengen gebruikt de gemeente de GAP-analyse, zelfevaluaties en externe audits.

2.2.1. De GAP-analyse geeft een beeld van de mate waarin de gemeente voldoet aan de BIO

De laatste jaarrapportage (2021) laat de GAP-analyse van 2019, 2020 en 2021 zien. Daarin zijn de 14 controls uit de BIO (H5 t/m 18) opgenomen en is percentagegewijs aangegeven in welke mate de gemeente voldoet aan de normering uit de BIO. Door de verschillende jaren over elkaar heen te plotten geeft het beeld in de jaarrapportage een weergave van de voortgang van de informatieveiligheid op verschillende processen in de gemeente.[26]

De monitoring laat zien dat er over de jaren 2019 - 2021 is gewerkt aan informatieveiligheid en dat er voortgang is geboekt op de verschillende controls uit de BIO. Naast de weergave waarin percentagegewijs is aangegeven in welke mate de gemeente voldoet aan de gestelde norm. Ook is voor iedere BIO-norm uitgeschreven wat de status is van de gemeentelijke organisatie op die norm.[27]

[26] Rapportage Gegevensbescherming en Informatiebeveiliging 2021.
[27] Rapportage Gegevensbescherming en Informatiebeveiliging 2021.

2.2.2. De gemeente voert verschillende zelfevaluaties uit

Naast de toetsing aan de BIO-normering heeft de gemeente in 2021 5 zelfevaluaties uitgevoerd met behulp van de ENSIA-toolkit. Deze zelfevaluaties geven een beeld van de status van informatieveiligheid van bijvoorbeeld de Basisregistratie personen (BRP), de Paspoortuitvoeringsregeling Nederland (PUN) en de Basisregistratie Adressen en Gebouwen (BAG).[28]

2.2.3. Externe audits door Audit Dienst Rijk

In 2019, 2020 en 2021 zijn de externe audits op de DigiD-aansluiting en de toegang tot SUWInet uitgevoerd door de Audit Dienst Rijk. Ook deze audits zijn een vorm van monitoring op de informatieveiligheid binnen de gemeente.[29] De audits zijn in alle drie de jaren positief afgerond.

2.3. Afspraken met externe ketenpartners

De standaard werkwijze bij Rijssen-Holten is dat er met verwerkers een verwerkersovereenkomst wordt gesloten. Dit is overeenkomstig de VNG standaard. Er zijn aanvullende afspraken gemaakt over bewustwording met ketenpartners die geen verwerker zijn. Zij blijven zelf verantwoordelijk voor het naleven van de AVG. De gemeente Rijssen-Holten controleert niet zelf naleving door ketenpartners.

Niet alle ketenpartners zijn echter verwerkers, waardoor afspraken met deze partners contractueel moeten worden vastgelegd, hetzij contractueel of in een ketenverband via convenanten omdat er geen verwerkersovereenkomst wordt opgesteld. Dit wordt momenteel beperkt gedaan. Wel wordt er momenteel gewerkt aan een contractenregister dat meer overzicht moet bieden in de lopende afspraken.

2.4. Vertaling en toepassing aanbevelingen uit 2017

In 2017 heeft de rekenkamer een onderzoek opgeleverd naar privacy en informatieveiligheid in het sociaal domein. Dit onderzoek bevatte 5 aanbevelingen:

Aanbevelingen uit 2017	Vertaling en toepassing aanbevelingen	Status
1. Maak afspraken met het college over de informatievoorziening over privacy- en informatiebeveiliging.	De gemeente heeft sinds 2017 heldere kaders voor informatiebeveiliging opgesteld (informatiebeveiligingsbeleid). Het privacybeleid is toe aan een evaluatie. Wel zijn er actuele protocollen en handvatten voor medewerkers.	
2. Scherp het beleid voor privacy aan, zodat het voldoende sturing geeft aan	Beide zijn uitgevoerd. De handvatten voor medewerkers in het sociaal domein zijn	

[28] Rapportage Gegevensbescherming en Informatiebeveiliging 2021.
[29] De onderzoekers hebben de jaarrapportages van 2019, 2020 en 2021 ingezien.

medewerkers in de praktijk en stel voor 1 januari 2018 het informatiebeveiligingsbeleid vast.	opgenomen in het gedragsprotocol. En het nieuwe informatiebeveiligingsbeleid is (weliswaar later dan in 2018) vastgesteld.	
3. Stel eenduidige werkprocessen vast en organiseer periodieke evaluaties met uitvoerende medewerkers.	Eenduidige werkprocessen zijn vastgelegd in het gedragsprotocol. De periode evaluaties met uitvoerende medewerkers vinden niet aantoonbaar structureel plaats.	
4. Monitor periodiek de stand van informatieveiligheid en stel op basis daarvan een actieplan op.	De gemeente voert zelfevaluaties uit, en laat externe toetsen uitvoeren.	
5. Maak afspraken met externe ketenpartners over: • de wijze waarop zij blijvende aandacht besteden aan bewustwording onder hun medewerkers; • de toezicht op en verantwoording over privacy en de informatieveiligheid.	De afspraken met ketenpartners zijn opgenomen in de verwerkersovereenkomsten. De afspraken worden niet gemonitord.	

3. Rol van de raad

Dit hoofdstuk richt zich op de informatiepositie van de gemeenteraad op het gebied van privacy en informatieveiligheid in het sociaal domein. Daarmee geeft dit hoofdstuk antwoord op de volgende deelvragen:

6. *Hoe wordt de raad geïnformeerd over het bereiken van doelstellingen met betrekking tot privacy en informatieveiligheid binnen het sociaal domein?*
7. *Wat is de kwaliteit van de informatievoorziening die de raad ontvangt?*

3.1. Informatievoorziening aan de raad

Jaarlijks stelt de gemeente de 'Jaarrapportage gegevensbescherming en informatiebeveiliging' op over het voorgaande jaar. Het college stelt deze jaarrapportage vast en ook de gemeenteraad ontvangt de jaarrapportage met daarbij een toelichtende raadsinformatiebrief. Deze rapportages zijn onderdeel van de P&C-cyclus van de gemeente.

In de jaarrapportages gegevensbescherming en informatiebeveiliging ontvangt de raad een verantwoording over het voorafgaande jaar. Met de jaarrapportages ontvangt de raad op de volgende punten informatie:[30]

- **Privacy en informatiebeveiliging:** De rapportage beschrijft de belangrijkste veranderingen en lopende processen. Ook is er aangegeven welke DPIA's er zijn uitgevoerd en welke ontwikkelingen er zijn op het gebied van externe samenwerking.
- **Informatieveiligheid:** Om een weergave te geven van de status van informatieveiligheid is de GAP analyse op basis van de BIO-normering opgenomen. Daarnaast is er een weergave opgenomen van de uitgevoerde zelfevaluaties met behulp van de ENSIA-toolkit en is er een weergave opgenomen van de extern uitgevoerde audits.
- **Bewustwording:** De rapportage gaat in op de belangrijkste ontwikkelingen op het gebied van bewustwording onder medewerkers op het thema gegevensbescherming.
- **Beveiligingsincidenten en datalekken:** De jaarrapportage geeft een overzicht van alle incidenten en datalekken die dat jaar hebben plaatsgevonden.
- **Collegeverklaring:** De collegeverklaring ENSIA is opgenomen in de jaarrapportage.
- **Verbetermaatregelen:** Tot slot bevat de jaarrapportage ook een overzicht van alle verbetermaatregelen om privacy en informatiebeveiliging beter te waarborgen.

Via de bijgaande raadsinformatiebrief voorziet het college de raad van een begrijpelijk uitleg van de ontwikkelingen op het gebied van gegevensbescherming en informatiebeveiliging. Buiten deze jaarrapportage als onderdeel van de P&C-cyclus heeft de raad geen rol en daardoor weinig betrokkenheid bij het onderwerp. Wel is er enig tijd geleden een bijeenkomst georganiseerd over een hack bij een buurgemeente, waarin de raad is meegenomen in de waarborgen en het beleid.

[30] De onderzoekers hebben de jaarrapportages van 2019, 2020 en 2021 ingezien.

4.Wetsontwikkeling

Dit hoofdstuk richt zich op de wetsontwikkeling van privacywetgeving in het sociaal domein sinds 2017. Daarmee geeft dit hoofdstuk antwoord op de volgende deelvraag:

8. *Hoe is de wetgeving sinds de uitvoering van het vorige onderzoek ontwikkeld en wat betekent dat voor de toekomst?*

4.1. Wetsontwikkelingen sinds 2017 – sociaal domein

Sinds de decentralisaties van 2015 hebben gemeenten meer verantwoordelijkheden gekregen binnen het sociaal domein, met name op het gebied van jeugdhulp en de Wet maatschappelijke ondersteuning (Wmo) 2015. Gemeenten worden geacht te streven naar een geïntegreerde samenwerking tussen professionals die verschillende domeinen overstijgt. De behoefte aan gegevensuitwisseling voor een geïntegreerde samenwerking kan soms in conflict zijn met de privacywetgeving, zoals vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). Na 2015 zijn er verschillende wetsontwikkelingen geweest op het gebied van privacy en het sociaal domein. De belangrijke wetsontwikkeling is bijvoorbeeld de Wet gemeentelijke schuldhulpverlening, zoals besproken in paragraaf 1.6.4 van deze rapportage.

4.2. Toekomstige wetsontwikkelingen – sociaal domein

4.2.1. Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams)

Het bieden van integrale ondersteuning in het sociaal domein met daarbij de benodigde domeinoverstijgende gegevensuitwisseling is vaak lastig voor gemeenten. Met het wetsvoorstel Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams) probeert de wetgever dit probleem te ondervangen door een duidelijke wettelijke basis te creëren voor de uitwisseling van gegevens die in zulke gevallen nodig is. Het wetsvoorstel, dat in de zomer van 2022 langs de Raad van State is geweest, betreft een wijziging van de Wet maatschappelijke ondersteuning (Wmo) en de relevante spiegelbepalingen in de Jeugdwet, Participatiewet en de Wet gemeenschappelijke schuldhulpverlening.[31] Deze wijziging moet helpen om gegevens uit te wisselen tussen het sociaal domein en de aanpalende domeinen: zorg en ggz, welzijn, onderwijs, wonen, openbare orde en veiligheid, werk en inkomen en inburgering.[32] De wetswijziging zou gemeenten vooral een extra instrument moeten geven om te werken aan integrale hulpverlening in het sociaal domein. In maart 2020 is het wetsvoorstel van de Wams ter consultatie gelegd.[33] Daaruit kwamen enkele kanttekeningen

[31] Het Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams) is begin 2023 bij de Tweede Kamer ingediend. De beoogde inwerkingtreding is 1 januari 2024.
[32] Concept Wet aanpak samenhangende meervoudige problematiek in het sociaal domein (Wams).
[33] VNG (2022), Wetsvoorstel aanpak meervoudige problematiek in het sociaal domein (Wams): https://vng.nl/artikelen/wetsvoorstel-aanpak-meervoudige-problematiek-in-het-sociaal-domein-wams.

naar voren ten aanzien van de toenemende verantwoordelijkheid van de gemeente ten opzichte van externe partijen. Verder heeft de Raad van State een advies uitgebracht waarin zij onder meer de noodzaak van deskundigheidsbevordering bij professionals benadrukt, waarmee zij onder andere doelt op gemeenten.

In de Gedragsprotocol Sociaal Domein gemeente Rijssen-Holten is al vooruitgelopen op de inwerkingtreding van de Wams.

4.2.2. Verzamelwet gegevensbescherming

In 2022 is de Verzamelwet gegevensbescherming naar de Tweede Kamer verstuurd. De Verzamelwet gegevensbescherming brengt onder meer een wijziging van enkele bepalingen uit de UAVG tot stand. Die wijzigingen zijn voor de gemeente met name relevant als het gaat om de uitoefening van de rechten van betrokkenen.

Artikel 5 van de UAVG bepaalt dat er voor de verwerking van persoonsgegevens van betrokkenen onder de 16 jaar toestemming nodig is van de wettelijke vertegenwoordiger. Dit blijft ook zo na de wetswijziging. De betrokkene die ouder is dan 12 maar jonger dan 16 krijgt echter het recht om de verleende toestemming in te trekken.[34] Daarnaast zal de wetswijziging jongeren van 12 jaar en ouder de mogelijkheid geven om zelfstandig de rechten uit hoofdstuk 3 van de AVG uit te oefenen. Dit betekent bijvoorbeeld dat jongeren vanaf 12 zich zelfstandig op het recht op rectificatie, inzage of vergetelheid kunnen beroepen zonder de instemming van hun wettelijk vertegenwoordiger. Verder zal rechtspositie van onder curatele staande en onder bewindvoering of mentorschap vallende betrokkene worden versterkt. Ook hier is er sprake van een uitbreiding van het recht om toestemming voor gegevensverwerking in te trekken.[35]

De wet brengt slechts beperkt wijzigingen aan in de werkwijze zoals verankerd in jeugdwet en WMO aangezien de domein-specifieke wetgeving blijft bestaan. Voor de gemeente zal deze wet dan ook beperkt effect hebben.

[34] De verankering van dit recht van de betrokkene zal in art. 5 lid 3 UAVG worden opgenomen.
[35] Zie: https://www.internetconsultatie.nl/verzamelwetgegevensbescherming voor het wijzigingsdocument van de UAVG als gevolg van de Verzamelwet gegevensbescherming.

Bijlage 1. Bronnenlijst

Bronnen

Voor bronvermeldingen verwijzen we naar de voetnoten in de lopende tekst.

Geïnterviewde personen

Tabel 1: Lijst met geïnterviewde personen, geanonimiseerd

Functie	Datum
Teammanager consulenten participatie	5 april 2023
Strategisch adviseur, voormalig adviseur kwaliteit sociaal domein	24 maart 2023
Indicatiesteller Wmo	24 maart 2023
Jeugdconsulent	21 maart 2023
Wethouder	7 november 2022
Functionaris Gegevensbescherming	7 november 2022
Informatievoorziening	7 november 2022

Bijlage 2. Afkortingen en begrippenlijst

Term	Toelichting
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.
Chief Information Security Officer (CISO)	De CISO is verantwoordelijk voor de implementatie van het informatiebeveiligingsbeleid en het toezicht op de uitvoering ervan.
ENSIA-systematiek	ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij overheidsorganisaties verder te professionaliseren door het toezicht te bundelen en aan te sluiten op hun eigen Planning & Control-cyclus.
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 privacy risico's van een gegevensverwerking in kaart te brengen. En om daarna maatregelen te kunnen nemen om de risico's te verkleinen.

Term	Toelichting
	Het is verplicht wanneer een gegevensverwerking waarschijnlijk een hoog privacy-risico 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.