Stappenplan privacybeleid sociaal domein

Waarom privacybeleid opstellen voor sociaal domein?

Om als gemeente integrale dienstverlening te kunnen bieden aan burgers in het kader van de drie decentralisaties is het kunnen delen van gegevens binnen en, indien noodzakelijk, over domeinen een randvoorwaarde. Burgers moeten erop kunnen vertrouwen dat er zorgvuldig wordt omgegaan met persoonsgegevens wanneer zij bepaalde zorg of dienstverlening ontvangen en dat dit binnen de kaders van de wet gebeurt.

Natuurlijk hebben gemeenten nu al de verantwoordelijkheid voor het goed en zorgvuldig omgaan met persoonsgegevens van burgers. De decentralisaties kunnen betekenen dat gemeenten meer gegevens zullen verwerken en/of meer zullen samen werken met andere partners. Dat roept andere vragen op bijvoorbeeld over het delen van gegevens tussen professionals in een wijkteam. In de aanloop naar 2015 is het dus zaak om privacybeleid te (her)formuleren en dit te implementeren in de werkprocessen, de governance en de training en opleiding van betrokken professionals en medewerkers.

Het privacybeleid beschrijft de doorvertaling van de generieke normen uit wet- en regelgeving naar de eigen gemeentelijke situatie. Het gaat daarbij zowel om de inhoud als ook om de organisatie van het beleid (governance). Privacybeleid is maatwerk, afhankelijk van de inrichtings- en beleidskeuzes die de gemeente maakt. Het (her)formuleren van het privacybeleid voor het sociaal domein maakt inzichtelijk hoe de gemeente vanaf 1 januari 2015 met de persoonsgegevens van haar burgers omgaat. Dit is belangrijk voor de verantwoording over het privacybeleid richting gemeenteraad, transparantie over het omgaan met gegevens richting de burgers en het geeft kaders voor de professionals die met de persoonsgegevens werken.

Dit stappenplan biedt handvatten over hoe je het privacybeleid van de gemeente kunt formuleren.

Stappenplan voor opstellen van lokaal privacybeleid

1. **Betrek de juiste personen bij het opstellen van het privacybeleid**

   Privacybeleid is zowel een zaak van het management en bestuur van de gemeenten omdat zij verantwoordelijk zijn voor inrichting en toezicht, als ook van de professionals binnen en buiten de gemeenten die zich moeten houden aan het privacybeleid. Het is belangrijk om bij het ontwikkelen van het beleid de juiste mensen te betrekken om te zorgen voor beleid dat uitvoerbaar is en draagvlak heeft. Natuurlijk is het ook van belang om juridische kennis te betrekken vanaf de start.

2. **Zorg dat je voldoet aan de wettelijke kaders rondom privacy**

   Voor het omgaan met persoonsgegevens van burgers is de WBP leidend. De WBP geeft het kader voor het goed en zorgvuldig omgaan met persoonsgegevens. Voor het sociaal domein zijn verder de verschillende materiewetten (Jeugdwet, WMO en Participatiewet) van belang. Tot slot is het van belang dat de eigen lokale kaders bekend zijn. Dat betreft zowel de eigen

gemeente als ook de partners waarmee samengewerkt wordt in het sociaal domein. Vragen zijn: zijn er binnen de gemeente al uitgangspunten geformuleerd voor borgen privacy van burgers? Wat is het privacybeleid van betrokken partners? Het is belangrijk om voort te bouwen op bestaande kennis. Denk daarbij aan bestaande samenwerkingsconvenanten of geformuleerd beleid met betrekking tot informatieveiligheid (zie voor meer informatie de website van de informatiebeveiligingsdienst voor gemeenten[1]).

3. **Lees de kabinetsvisie "Zorgvuldig en bewust: gegevensverwerking in een gedecentraliseerd sociaal domein"[2]**

De Beleidsvisie "Zorgvuldig en bewust: gegevensverwerking en privacy in een gedecentraliseerd sociaal domein" is nu beschikbaar. Deze kabinetsvisie is opgesteld door het ministerie van BZK in overleg met de ministeries van VWS, VenJ, SZW, OCW en de VNG. De beleidsvisie geeft richtlijnen voor gemeenten voor het zorgvuldig omgaan met persoonsgegevens in het kader van decentralisaties.

In de kabinetsvisie is gebouwd op drie pijlers: balans tussen noodzakelijke gegevensverwerking vanuit de maatschappelijke opgave in het sociaal domein en borging van de privacy, versterking van de positie van de bewoner, en versterken van de democratische verantwoording over gegevensverwerking en privacy op lokaal niveau. De kabinetsvisie kan helpen bij het ontwikkelen van de gemeentelijke visie. **Vertaal het inhoudelijk beleid en inrichtingskeuzes in het sociaal domein naar wat dat betekent voor de privacy van de burger.** Het inhoudelijk beleid en de daaruit voortkomende inrichtingskeuzes in het nieuwe sociale domein bepalen de verdere inrichting van het privacybeleid in het sociaal domein. Uw visie op de maatschappelijke opgave van uw gemeente is daarbij tevens uitgangspunt. Voor inrichtingskeuzes met betrekking tot het sociaal domein kunt u gebruik maken van de Archetypen die binnen het VISD-programma zijn beschreven.

Neem in het lokale privacybeleid in elk geval de volgende punten op:

Visie: De privacy van de burger in relatie tot de maatschappelijke opgave in het sociaal domein. Welke uitgangspunten worden gehanteerd? Welke keuzes worden gemaakt? Welke dilemma's zijn er?[3]

- Governance: zoals de verantwoording aan de Gemeenteraad, wijze van inrichting en controle op waarborgen privacy, inclusief de functionaris gegevensverwerking als interne toezichthouder, de afspraken met derden (leveranciers/samenwerkingspartners/derden) inclusief de verantwoording door hen.
- Organisatorische borging van de privacy: mandatering van taken, kennis en bewustwording van medewerkers, expertondersteuning over privacy voor medewerkers, sturing en monitoring (indicatoren).

[1] Zie de website van de IBD
[2] http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/05/27/kamerbrief-over-de-beleidsvisie-privacy-in-sociaal-domein.html
[3] Denk bijvoorbeeld aan keuzes met betrekking tot zelfregie/zelfredzaamheid burgers in relatie tot regie gemeenten. Of vroegsignalering. De visie van de gemeente op de maatschappelijke opgave bepaalt mede de wijze waarop privacybeleid binnen gemeente vorm en inhoud krijgt.

- Samenwerking en uitbesteding: eisen die je aan samenwerkingspartners stelt om de privacy te borgen.
- Werkprocessen: omgang met gegevens, waarborgen voor de privacy, triagemomenten[4], vroegsignalering.
- ICT-systemen en informatieveiligheid: eisen die je vanuit privacy- en informatieveiligheidsperspectief moet stellen aan de gegevensverwerking, bewaren en vernietigen van gegevens.
- Positie en rechten van de burger: De rechten zoals het opvragen van de eigen gegevens, klachten afhandeling en ook hoe je als gemeente met de burger wilt omgaan in relatie tot de privacy (hoe wordt de burger hierover geïnformeerd, inclusief ombudsfunctie.

VOORBEELD GEMEENTE LEEUWARDEN

De beleidsuitgangspunten ten aanzien van de bescherming van persoonsgegevens in Leeuwarden zijn:

- De hulpvraag van de bewoner is leidend. Ook als het gaat om verwerken of delen van informatie (persoonsgegevens van de bewoner) is de hulpvraag van de bewoner leidend. De informatie die verwerkt of gedeeld wordt is dus altijd gerelateerd aan die hulpvraag.
- De bewoner wordt altijd geïnformeerd over wat er met zijn of haar informatie gebeurd en waarom. Er wordt dus uitgegaan van het transparantiebeginsel[1].
- Leeuwarden wil door de inzet en zichtbaarheid van de sociaal werker in de wijk problemen of vragen vroegtijdig signaleren. Dit gebeurt dus niet op basis van het raadplegen van bronnen of risicoprofielen.
- Leeuwarden gaat uit van de professionaliteit van de sociaal werkers. De sociaal werkers maken dus per casus een afweging over de doelbinding, proportionaliteit en subsidiariteit als het gaat om het verwerken of delen van persoonsgegevens van de bewoner. Dit wordt beschreven in de triageprocessen en de afweging (argumenten en het resultaat) wordt vastgelegd in het regiesysteem.
- De benodigde gegevensverwerking ten behoeve van de vraagverheldering en het opstellen van het plan van aanpak wordt in principe samen met de bewoner bepaald en uitgevoerd. Zo is de regel dat de betrokken bewoner aanwezig is bij het zorgoverleg over zijn/haar plan van aanpak.
- Alleen de sociaal werker heeft toegang tot het volledige dossier.
- De sociaal werker verwerkt alleen de zogenoemde DAT-informatie van ketenpartners die een deelactiviteit van het plan uitvoeren. Detailinformatie over de geleverde zorg en de bewoner blijft bij de ketenpartner.

4. Laat een jurist het geformuleerde beleid toetsen

Laat een jurist het beleid toetsen om zo er zeker van te zijn dat dit strookt met de juridische kaders (de verschillende materiewetten en de Wbp) en of het aansluit bij het bestaande privacybeleid van de gemeente.

5. Laat de gemeenteraad het privacybeleid vaststellen

[4] Zie Factsheet Triage https://www.visd.nl/sites/visd/files/Factsheet-Privacy-Triage-Sociaal-Domein-versie-0-6-juni-2014.pdf

6. Zorg dat het geformuleerde privacybeleid de basis is voor de verdere uitwerking van privacy-bouwstenen.

Wanneer het privacybeleid geformuleerd is dan kan dit dienen als input voor:

- Afspraken die er over privacy gemaakt worden met derden (bijvoorbeeld de ICT-leverancier, een organisatie waaraan specifieke taken zijn uitbesteed of ketenpartners);
- Communicatie over privacy richting de burger;
- Een gedragscode en werkinstructie over privacy voor de professionals in het sociaal domein.