PRIVACY GOVERNANCE BINNEN HET SOCIAAL DOMEIN

Inhoudsopgave

Privacy Governance binnen het Sociaal Domein 1
HOOFDSTUK 1 doel en opzet van dit document 3
1.1 Doel 3
1.2 Opzet document 3
HOOFDSTUK 2 De verantwoordelijkheid van de gemeente 3
2.1 Nieuwe taken en nieuwe rol gemeenten 3
2.2. Regie en samenwerking 3
2.3 Verantwoordelijkheid bij uitbesteden taken 4
2.4 Het College van B&W is verantwoordelijk 4
Hoofdstuk 3 Governance intern 4
3.1 Stappenplan voor het inrichten van de governance intern 4
3.2 Benoem een regievoerder privacy sociaal domein 5
3.3 Beschrijf de rollen en verantwoordelijkheden privacy sociaal domein wiens verantwoordelijkheid zou dit moeten zijn? 5
3.4 Maak afspraken over de verantwoording aan de Gemeenteraad: 7
Hoofdstuk 4 Governance extern 8
4.1 Stappenplan governance extern 8
4.2 Breng alle externe stakeholders in kaart 8
4.3 Geef per stakeholder aan op welke manier wordt samengewerkt 8
4.3. Inventariseer alle bestaande afspraken 8
4.4. Bepaal met welke stakeholders afspraken moeten worden gemaakt of aangepast 8
Bijlage 1 – Voorbeeld Functieprofiel Functionaris Gegevensbescherming 10

HOOFDSTUK 1 DOEL EN OPZET VAN DIT DOCUMENT

1.1 Doel

Het doel van dit document is om de gemeente informatie en handvatten te bieden voor het inrichten van de privacy governance in het sociaal domein. Gemeenten moeten uiteraard altijd al zorgvuldig omgaan met persoonsgegevens van burgers. Maar doordat er in 2015 veel taken in het sociaal domein bij zijn gekomen is het voor gemeenten een goed moment om bij de inrichting en doorontwikkeling van het sociaal domein direct de rollen, verantwoordelijkheden en taken met betrekking tot privacy te beleggen en goede afspraken te maken met externe partijen over de zorgvuldige omgang met persoonsgegevens. In het raamwerk Privacy van de VNG wordt governance aangemerkt als een van de aandachtsgebieden voor gemeenten. Om privacy te borgen is het van belang dat er in de lijnorganisatie aandacht is voor het onderwerp. De gegevensverwerking in het sociaal domein voor de gemeentelijke taken gebeurt onder verantwoordelijkheid van het College van B&W. Zij moet daarover verantwoording afleggen aan de gemeenteraad stelt het Kabinet in de visie op privacy en gegevensuitwisseling in het sociaal domein "Zorgvuldig en bewust"[1]. Dit betekent dat die verantwoording in de eigen (of gemeentelijke) organisatie moet worden belegd én dat er afspraken gemaakt moeten worden met samenwerkingspartners. Deze notitie geeft handvatten over hoe je dat kan doen en waar je op moet letten als het gaat om goed inrichten van de interne en externe privacy governance. Dit document staat niet op zichzelf maar is een aanvulling op de andere instrumenten en handreikingen die horen bij het privacy raamwerk van de VNG. [2]

1.2 Opzet document

In dit document gaan we in op (1) de verantwoordelijkheid van de gemeente voor een zorgvuldige omgang met persoonsgegevens, en behandelen we achtereenvolgens (2) het inrichten van de governance intern en (3) het inrichten van de governance extern. In de bijlage is een voorbeeld opgenomen van een functieprofiel voor de Functionaris Gegevensbescherming.

HOOFDSTUK 2 DE VERANTWOORDELIJKHEID VAN DE GEMEENTE

2.1 Nieuwe taken en nieuwe rol gemeenten

Door de drie decentralisaties hebben gemeenten omvangrijke nieuwe taken in het sociaal domein. De gemeente is verantwoordelijk voor de goede uitvoering van al deze wettelijke taken. Onderdeel van een goede uitvoering is een zorgvuldige omgang met persoonsgegevens.
Integraliteit is een belangrijke doelstelling van de decentralisaties in het sociaal domein: gemeenten mogen indien noodzakelijk over de grenzen van sectoren in het sociaal domein heen kijken en mogen dus ook persoonsgegevens uit verschillende sectoren bij elkaar brengen als de urgentie van de situatie dat vraagt. In de materie wetten (Jeugd, WMO, Participatiewet) is beschreven welke taken de gemeente heeft en welke eisen er worden gesteld aan gegevenswerking. Op het moment dat er integraal of domeinoverstijgend wordt gewerkt, is in aanvulling op die materiewetten de WBP (Wet bescherming persoonsgegevens) van toepassing.

2.2. Regie en samenwerking

Binnen het sociaal domein werkt de gemeente vanuit haar regierol samen met aanbieders en hulpverleners om een bepaalde zorg, voorziening of dienstverlening aan te bieden aan de betrokkene(n). Samenwerking kan alleen met inachtneming van ieders positie en verantwoordelijkheden. De gemeente zorgt ervoor dat afspraken worden gemaakt met de samenwerkingspartijen over zorgvuldige gegevensverwerking en privacy. Denk hierbij aan een samenwerkingsconvenant die de betrokken jeugdhulpinstelling, medische hulpverleners, onderwijsinstellingen en/of woningcorporaties dienen te ondertekenen.

---

[1] Kabinetsvisie: Zorgvuldig en bewust (Rijksoverheid, download)

[2] VNG dossier ISD – Privacy en gegevensuitwisseling

2.3 Verantwoordelijkheid bij uitbesteden taken

Bij de uitbesteding van taken aan private partijen, zoals ICT leveranciers, zorgverleners, of (o.a. afhankelijk van de gekozen organisatievorm) een wijkteam, blijft de gemeente verantwoordelijk voor de goede uitvoering van die taken. Dat betekent ondermeer dat de gemeente de eisen omtrent de gegevensverwerking moet borgen in contracten met derde partijen, zoals inkoopcontracten en convenanten, en bv. de mogelijkheid voor het uit laten voeren van een privacy-audit binnen de uitbesteedde partij. Overigens hebben deze partijen ook een eigen verantwoordelijkheid ten aanzien van privacy, bijvoorbeeld als bewerker in de zin van de WBP.

2.4 Het College van B&W is verantwoordelijk

Het College van B&W is verantwoordelijk voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaats vindt en kan eisen stellen aan de beveiliging en borging van de privacy. Het College is voor de wijze waarop het hieraan invulling geeft verantwoording verschuldigd aan de Gemeenteraad. Dit betekent dat er goede afspraken moeten worden gemaakt op welke manier de verantwoording aan de Raad plaatsvindt.

HOOFDSTUK 3 GOVERNANCE INTERN

Om bij de inrichting en doorontwikkeling van het sociaal domein de privacy van burgers direct te kunnen borgen is het van belang om de rollen en verantwoordelijkheden te bepalen rondom de zorgvuldige omgang met persoonsgegevens. Binnen de organisatie moet in kaart worden gebracht wie waarvoor verantwoordelijk is: wat is de rol van bedrijfsvoering, teammanagers, kwaliteitsmedewerkers, professionals, de afdeling communicatie, informatiebeveiliging etc.? Hierbij moet ook duidelijk worden aangegeven op welke manier de betreffende medewerkers over het thema privacy rapporteren zodat dit kan worden meegenomen in de verantwoording richting gemeenteraad[3] Dit kan bijvoorbeeld meegenomen worden in een jaarverslag door de afdeling bedrijfsvoering en teammanagers kunnen hier met de professional tijdens casusbesprekingen of intervisie met collega's aandacht aan besteden.

3.1 Stappenplan voor het inrichten van de governance intern

Het is aan te bevelen de volgende stappen te nemen om de privacy governance intern in te richten. De stappen worden hieronder nader toegelicht.

Aandachtspunten

- Maak bij het beschrijven van de rollen en verantwoordelijkheden duidelijk een onderscheid tussen bestuurlijke eindverantwoordelijkheid (dit is het College van B&W) en ambtelijke eindverantwoordelijkheid.
- Het is mogelijk om regionaal één Functionaris Gegevensbescherming aan te stellen die toezicht houdt op het thema privacy in meerdere gemeenten, maar die persoon moet wel goed op de hoogte zijn van de verschillende inrichtingsvarianten en daar rekening mee kunnen houden bij de uitvoering van zijn taken.
- Betrek het College al in een vroeg stadium bij het formuleren van privacybeleid en zorg dat de urgentie op het thema in de gemeente breed wordt gevoeld.

[3] Handreiking Verantwoording privacy sociaal domein aan de gemeenteraad (VNG/KING, oktober 2015, pdf)

3.2 Benoem een regievoerder privacy sociaal domein

Het is aan te bevelen om iemand in de gemeente aan te stellen die (tijdelijk) de regie voert op de borging van privacy in het sociaal domein. Dit zou een Functionaris voor de gegevensbescherming (FG) kunnen zijn, maar dit is niet verplicht. Het is in ieder geval van belang dat deze medewerker de ontwikkeling, implementatie en operationele uitvoering overziet van het privacybeleid binnen de gemeente. Dit beleid richt zich niet alleen op de medewerkers, maar ook op de communicatie en relatie met de burger. De regievoerder privacy sociaal domein heeft hierin een adviserende en toezichthoudende functie binnen de gemeente. In de praktijk wordt deze rol op verschillende wijzen ingericht. Soms wordt de taak belegd bij informatievoorziening (informatiebeveiliging) soms bij juridische zaken en in sommige gevallen bij een medewerker kwaliteit. De invulling van de rol kan dus verschillen per organisatie.

3.3 Beschrijf de rollen en verantwoordelijkheden privacy sociaal domein wiens verantwoordelijkheid zou dit moeten zijn?

Het is belangrijk om de rollen en verantwoordelijkheden in het sociaal domein te beschrijven om inzichtelijk te krijgen wie er persoonsgegevens verwerkt en bijvoorbeeld wie welke autorisaties er bij de rol horen. Deze beschrijving kan het best gemaakt worden door de privacyverantwoordelijke (de functionaris gegevensbescherming of een projectgroep privacy) in combinatie met degene die verantwoordelijk is voor de uitvoering van het sociaal domein. Elke gemeente richt het sociaal domein op haar eigen manier in. De voorbeelden van rollen en verantwoordelijkheden hieronder zijn bedoeld om een indruk te geven en zullen niet altijd één op één overeenkomen met de functies binnen uw eigen gemeente.

Functionaris voor de gegevensverwerking

De functionaris voor de gegevensverwerking wordt door het College Bescherming Persoonsgegevens (CBP) omschreven als de onafhankelijke toezichthouder voor de toepassing en de naleving van de Wet Bescherming Persoonsgegevens (Wbp) binnen organisaties of branches. Deze specifieke rol is niet verplicht. Het CBP bevordert wel de aanstelling van een interne toezichthouder, aangezien zelfregulering en integratie van het toezicht in de normale bedrijfsvoering een effectieve bijdrage levert aan het realiseren van een betere bescherming voor de persoonsgegevens. Het is mogelijk dat deze activiteiten en verantwoordelijkheden die hier zijn omschreven belegd worden bij iemand die ook andere taken heeft. Om ervoor te zorgen dat de FG zijn rol zo onafhankelijk mogelijk uit kan voeren wordt zeer aangeraden dat de FG een onafhankelijke staffunctie bekleedt (en direct aan het verantwoordelijke college binnen de organisatie te rapporteert. De functie van FG is een lastige omdat het in de eigen organisatie ook controleert en anderen moet kunnen aanspreken op bijvoorbeeld bovenmatig verwerken van persoonsgegevens. Daarom is het van belang dat gewaarborgd wordt dat deze persoon zijn of haar werk goed kan doen. Het Wbp stelt een aantal eisen aan deze interne toezichthouder. Ten eerste moet de FG een natuurlijk persoon zijn. Ten tweede, dient een FG betrouwbaar te zijn en dermate politiek vaardig te zijn dat hij in staat is om zijn belangen van verschillende partijen tegen elkaar af te kunnen af wegen.

Tot de werkzaamheden van een FG behoren bijvoorbeeld:

- toezicht houden
- verzamelen van inventarisaties van gegevensverwerkingen
- het bijhouden van meldingen van gegevensverwerkingen
- klachtenbehandeling
- voorlichting
- het ontwikkelen van interne regelingen
- adviseren over technologie en beveiliging

Een belangrijke taak van de FG is om ervoor te zorgen dat vragen over de wijze waarop er door de organisatie wordt om gegaan met persoonsgegevens en eventuele klachten over het gebruik van persoonsgegevens af te handelen. Door deze werkzaamheden kan het noodzakelijk zijn dat de FG persoonsgegevens van betrokkenen in ziet.

Klant Contact Centrum (KCC)

Het Klant Contact Centrum is één van de klantingangen waar burgers terecht kunnen voor vragen, aanvragen en meldingen. Als belangrijk contactpunt met de burger is het mogelijk dat zij informatie ontvangen die van belang kunnen zijn voor de klachtencoördinator en de functionaris voor de gegevensverwerking. Zij dienen in staat te zijn om klachten en meldingen met betrekking tot gegevensverwerking en privacy naar hen door te

zetten. Het KCC heeft daarom een belangrijke rol in het doorverwijzen van deze vragen en meldingen naar de relevante contactpersonen.

Klachtencoördinator (KC)
De klachtencoördinator is verantwoordelijk voor activiteiten zoals het afhandelen, c.q. uitzetten en monitoren, van verzoeken tot inzage, verbetering, aanvulling, verwijdering of afscherming, het recht van verzet en het afhandelen van klachten. De klachtencoördinator informeert de FG over het aantal klachten, aard van de klachten en voortgang van de afhandeling. Afhankelijk van de zwaarte van de FG rol en of de rol van klachtencoördinator in de gemeente al wordt vervuld, is het een mogelijkheid om deze rol bij de FG onder te brengen.

Afdelingshoofd Sociaal Domein (ASD)
Een afdelingshoofd is verantwoordelijk voor de teams en heeft daardoor een verantwoordelijkheid als het gaat om het borgen van de privacy in de werkprocessen van de professionals of in de uitvoering. Het afdelingshoofd moet bijvoorbeeld zorg dragen voor de privacy bewustwording van professionals in een wijkteam en informeert de KC en FG wanneer dit nodig is. Het afdelingshoofd legt, afhankelijk van de inrichting en organisatiestructuur binnen de gemeente, verantwoording af aan het College van B&W. Wanneer de aansturing van de wijkteams op een andere manier georganiseerd is zal de verantwoordelijkheid dus ook bij een andere functionaris kunnen liggen.

Teammanager
De teammanager is de coördinator van het team en is verantwoordelijk dat het team het privacybeleid van de gemeente bij het uitvoeren van de taken naleeft. Afhankelijk van de grootte van het team en de rol van de teamleider is het mogelijk dat deze een coördinerende rol speelt in casusoverleggen en daardoor toegang krijgt tot persoonsgegevens. De teammanager kan ook een belangrijke rol spelen in het creëren van privacy-bewustzijn bij medewerkers en bijvoorbeeld het organiseren van intervisie over privacydilemma's.

Regisseur/ sociaal werker
De sociaal werker (of casusregisseur) is het aanspreekpunt rond een gezin, persoon of huishouden en is verantwoordelijk voor het opstellen van, indien nodig, één samenhangend plan en het coördineren van de uitvoering hiervan. In de uitvoering van het plan signaleert de regisseur wat er wel en niet goed gaat, 'Makelt en schakelt' en intervenieert waar nodig. De regisseur is verantwoordelijk voor de afstemming hiervan met andere hulpverleners die betrokken zijn bij het plan. In de praktijk kan de sociaal werker de rol van regisseur op zich nemen. De regisseur/ sociaal werker is de professional die in contact staat met het gezin en daarmee persoonsgegevens opvraagt, verwerkt en eventueel deelt. Het is van belang dat deze professionals zich bewust zijn van het belang van de bescherming persoonsgegevens en hierin worden getraind. Zij maken op verschillende momenten in het proces een afweging (triage) over het doel waarmee ze informatie delen, opvragen of bewerken (doelbinding). Deze afwegingen noemen we triage momenten (zie ook factsheet triage[4] en triage-instrument) Het is ook belangrijk dat duidelijk is waar er sprake is van een taak op het gebied van toeleiding naar de hulpverlening of dat er zelf hulpverlening wordt geboden. Dit kan consequenties hebben voor de eisen die er aan de gegevensverwerking worden gesteld (bijvoorbeeld in het kader van de jeugdwet, zie ook PIA Jeugd [5]).

Vrijwilliger
Een vrijwilliger kan taken uitvoeren ter ondersteuning van het team. Afhankelijk van de taken van de vrijwilliger is het mogelijk dat deze toegang kan krijgen tot persoonsgegevens. Het is dan ook van belang dat niet alleen de medewerkers van het team een geheimhoudingsverklaring tekenen (zij hebben al beroepsgeheim of een afgeleid beroepsgeheim), maar ook de vrijwilligers die toegang hebben tot persoonsgegevens of deze verwerken. Het takenpakket van de vrijwilliger wordt bepaald door de teamleider.

Administratieve ondersteuning
De persoon die de rol van Administratieve ondersteuning vervult, ondersteunt de teamleider en teamleden in praktische onderdelen binnen de operatie.

[4] Factsheet Triage ISD Programma (VNG/KING, september 2015)
[5] Privacy Impact Assessment (Privacy Care, oktober 2014, pdf)

Informatie Beveiligingscoördinator (IBC)
De informatie beveiligingscoördinator is degene die onder het gezag van de verantwoordelijke belast is met de verantwoordelijkheid voor de informatiebeveiliging. Tot de taken behoren onder meer het opstellen van het informatiebeveiligingsplan en het bewaken van dit plan. Daarnaast adviseert hij het management en/of directie over beveiliging, mogelijke risico's en de daarbij horende mitigerende maatregelen. De IBC inventariseert en rapporteert over beveiligingsincidenten aan het management / directie. De FG en de IBC werken nauw samen om ervoor te zorgen dat er passende technische en organisatorische maatregelen worden genomen op het gebied van de verwerking van persoonsgegevens.

Applicatiebeheerder (AB)
De applicatiebeheerder is de persoon die verantwoordelijk is voor het functioneel beheer van de systeemapplicaties binnen de gemeente of het wijkteam. De AB heeft als taak om het beveiligingsbeleid dat is opgesteld door de IBC operationeel uit te voeren. Onderdeel van dit beleid is het configureren en toezicht houden op de autorisaties binnen de systemen. Deze persoon dient als aanspreekpunt voor het management en gebruikers omtrent de applicaties en als tussenpersoon richting de beheerder of softwareleverancier(s).

De Gemeenteraad
De Raad is in haar kaderstellende rol verantwoordelijk om het proces voor de afweging ten aanzien van gegevensverwerkingen en het afwegingskader te bekrachtigen. Daarnaast controleert de Raad het college B&W op haar verantwoordelijkheid betreffende de zorgvuldige verwerking van persoonsgegevens door of namens de gemeente.

College van Burgermeester & Wethouders
In de Beleidsvisie Privacy Sociaal Domein is beschreven dat het college van B&W verantwoordelijk is voor de zorgvuldigheid van de gegevensverwerking die door of namens de gemeente plaatsvindt. Dit betekent dat het College dient te zorgen voor een zorgvuldig geïmplementeerd triage proces en de borging van privacy in het sociaal domein. Daartoe maakt zij afspraken met samenwerkingspartners over de zorgvuldige verwerking van persoonsgegevens. Het College heeft binnen de gemeente dan ook een toezichthoudende rol om zorg te dragen dat persoonsgegevens op een zorgvuldige manier worden verwerkt. Deze rol zou dus bij iedere gemeente belegd moeten worden zodat hier uitvoering aan kan worden gegeven en het college daardoor verantwoording kan afleggen aan de Gemeenteraad. Het College legt daarbij verantwoording af aan de Gemeenteraad om ervoor te zorgen dat de uitvoering zichtbaar, controleerbaar en evalueerbaar plaatsvindt.

3.4 Maak afspraken over de verantwoording aan de Gemeenteraad:
Het college van B&W dient verantwoording af te kunnen leggen over de wijze waarop de gemeente de privacy van haar burgers in het sociaal domein waarborgt. Het is aan te raden hierover afspraken te maken met de Gemeenteraad en de rapportage in te richten op basis van Privacy raamwerk van de VNG[6]:

- Beleid: Geef aan waar eventuele wijzigingen of aanvullingen op het beleid (door voortschrijdend inzicht) zijn
- Governance: Neem in de rapportage mee op met welke partijen er afspraken gemaakt zijn over de verwerking van persoonsgegevens in het sociaal domein. Beschrijf ook de afspraken die zijn gemaakt over de verantwoording aan de gemeente
- Werkprocessen en triage: Geef een korte toelichting op hoe Triage is verankerd in het werkproces, inclusief de manier waarop besluitvorming wordt vastgelegd
- Bewustwording en training: Geef aan hoe de professionals in het sociaal domein bewust gemaakt worden van hun verantwoordelijkheid, geef aan hoe er met burgers gecommuniceerd wordt, rapporteer over de aard, omvang en afhandeling van eventuele klachten
- Beheer en opslag gegevens: Geef kort aan hoe u het beheer en de opslag van gegevens veilig hebt georganiseerd. Sluit daarbij aan bij (rapportages met betrekking tot) Informatieveiligheidsbeleid van de gemeente

[6] VNG dossier ISD - Privacy en gegevensuitwisseling

HOOFDSTUK 4 GOVERNANCE EXTERN

In het sociaal domein werkt de gemeente veel samen met externe partijen. Ook organiseren sommige gemeenten de regierol door het uitbesteden van deze taak en de bijbehorende gegevensverwerking aan een private partij. Gemeenten blijven in dergelijke constructies altijd verantwoordelijk voor de zorgvuldige omgang met persoonsgegevens, zowel in politieke zin als in de zin van de Wbp. Daarom moet de gemeente met alle partners in het sociaal domein goede afspraken maken.

4.1 Stappenplan governance extern

Het is aan te bevelen de volgende stappen te nemen om de privacy governance intern in te richten. De stappen worden hieronder nader toegelicht.

4.2 Breng alle externe stakeholders in kaart

Breng in kaart met wie de gemeente samenwerkt in het sociaal domein.

4.3 Geef per stakeholder aan op welke manier wordt samengewerkt

Er zijn verschillende samenwerkingspartners in het sociaal domein:

- Partijen aan wie gemeentelijke taken worden uitbesteed (gemandateerd): het College van B&W blijft verantwoordelijk (in de zin van de WBP en politiek) verantwoordelijk.
- Partners bij wie hulp en dienstverlening wordt ingekocht. De partners die zorg en hulpverlening leveren/uitvoeren zijn verantwoordelijk voor de zorgvuldige gegevens verwerking op basis van de eigen taken/juridische kaders.
- Partners met wie wordt samengewerkt op casusniveau, bijvoorbeeld met politie, justitie, woningbouwvereniging etc.

4.3. Inventariseer alle bestaande afspraken

Ga per stakeholder na of in convenanten, bewerkersovereenkomsten of andere overeenkomsten afspraken zijn gemaakt over de zorgvuldige omgang met persoonsgegevens.

4.4. Bepaal met welke stakeholders afspraken moeten worden gemaakt of aangepast

Bepaal welke convenanten of andere overeenkomsten moeten worden aangepast en met welke partijen nog afspraken moeten worden gemaakt over de zorgvuldige omgang met persoonsgegevens in het kader van samenwerking in sociaal domein. Voor de verschillende samenwerkingspartners gelden andere afspraken:

<u>Aandachtspunten bij de afspraken met partijen aan wie gemeentelijke taken worden uitbesteed:</u>

- Doel van de samenwerking en de grondslagen van partijen op basis waarvan gegevens worden gedeeld – De verschillende niveaus van regie, en de positie van de regisseur(s) als spil in het proces van dienstverlening, en in het proces van gegevensverwerking.
- Het triageproces en de wijze waarop afwegingen ten aanzien van gegevensverwerking daarin een plaats hebben.

- De voorwaarden om gegevens uit te wisselen tussen instanties zonder toestemming van betrokkenen en een afwegingskader voor verwerken van gegevens in het kader van het vitaal belang (of een conflict van plichten).
- Hoe om te gaan met 'botsende logica's'. Hiermee worden situaties bedoeld waarin professionals vanuit andere taken (justitie versus jeugdzorg bijvoorbeeld) een andere afweging maken ten aanzien van de noodzaak om informatie te delen, waardoor patstelingen kunnen ontstaan op de werkvloer.
- De overdracht van gegevens bij overgang naar een andere vorm van ondersteuning
- De manier waarop de burger actief geïnformeerd wordt over zijn of haar rechten met betrekking tot gegevensdeling
- Het omgaan en melden van vroege signalen
- Procedures bij personele wijzigingen
- Hoe men rapporteert aan de gemeente over de zorgvuldige gegevensverwerking
- Op welke manier de partij geaudit kan worden
- In welk systeem de gegevens staan, waar wordt het systeem gehost, wie is de eigenaar van de gegevens

Daarnaast zullen de afspraken in ieder geval het niveau van informatiebeveiliging moeten vastleggen (dat minimaal op hetzelfde niveau zal moeten plaatsvinden als neergelegd in de BIG) en de continuïteit van dienstverlening (bv. bij storingen en/of faillissement) moeten garanderen. De afspraken van de gemeente met samenwerkingspartners over het verwerken van gegevens zijn openbaar en komen transparant tot stand, de cliëntenraden hebben hierbij een adviserende rol.

<u>Aandachtspunten bij afspraken met partners bij wie hulp en dienstverlening wordt ingekocht:</u>

In bestekteksten of inkoopcontracten kan naar een zorgvuldige omgang met persoonsgegevens verwezen worden. Maak afspraken over:

- De uitwisseling (of beperking daarvan) van gegevens in de back office/ factureringsproces
- De eventuele samenwerking op casus niveau bij complexe problematiek (zie onderstaande)

<u>Aandachtspunten bij afspraken met partners met wie wordt samengewerkt op casusniveau</u>
Met partners met wie wordt samengewerkt op casusniveau, ook uit andere domeinen (bijvoorbeeld met politie, justitie, woningbouwvereniging etc.), worden vaak in samenwerkingsconvenanten de volgende afspraken worden gemaakt:

- Over signalen en meldingen:
    - De melder informeert de burger over de melding of niet indien niet mogelijk of niet wenselijk
    - Beperk de informatie die men meestuurt door alleen het signaal of melding te vermelden (maak bijvoorbeeld een uniform formulier voor meldingen/signalen)
    - Maak duidelijk onderscheid tussen melding bij Jeugd/wijk/WMO- team en meldingen aan Veilig Thuis (AMHK en Meldpunt Kindermishandeling)

- Over samenwerking bij multiprobleem casuïstiek (met Veiligheidshuis, OM, Politie, Reclassering, woningbouwcorporaties, jeugdzorginstellingen, maatschappelijk werk etc.) Besteed daarbij aandacht aan:
    - Triage (zie ook de publicatie Triagekader en instrument)
    - Informeren burger
    - Definities (wat is complex of multiprobleem)
    - Wanneer wordt wel en wanneer niet samengewerkt/gegevens uitgewisseld en op welke gronden/welke grondslagen hebben partijen en welke uitwisseling is wel/niet noodzakelijk
    - Regie (wie voert de regie over de casus, eventueel opschalen naar het Veiligheidshuis)
    - Botsende logica's (hoe ga je om met de verschillende wettelijke taken en kaders tussen de verschillende beleidsterreinen)

BIJLAGE 1 – VOORBEELD FUNCTIEPROFIEL FUNCTIONARIS GEGEVENSBESCHERMING

Doel

De Functionaris voor de gegevensverwerking (FG) overziet de ontwikkeling, implementatie en operationele uitvoering van het privacy beleid binnen de gemeente. Dit beleid richt zich niet alleen op de medewerker, maar ook op de communicatie en relatie met de burger. De FG heeft hierin een adviserende en toezichthoudende functie binnen de gemeente.

Kerncompetenties

1. Toereikende kennis

De FG heeft kennis van de regels voor de bescherming van persoonsgegevens. Het gaat hier niet alleen om de Wet Bescherming Persoonsgegevens(Wbp), maar ook sectorspecifieke regelgeving is hierin noodzakelijk. De kennis die noodzakelijk is voor de rol van FG beperkt zich niet tot het juridische vlak. Het is van belang dat de FG ook deskunding is op het gebied van informatie- en communicatie technologie. Hij kan gezien worden als de brug tussen juridische vakkennis en informatie technologie.

2. Betrouwbaar

Het is niet ongebruikelijk dat de FG in situaties terecht komt waarin hij vertrouwelijke informatie over betrokkenen onder ogen krijgt om een advies te kunnen geven. Daarnaast komt hij in zijn toezicht en controlerende rol regelmatig in contact met vertrouwelijke persoons- en gemeentelijke informatie. Betrouwbaarheid en zorgvuldigheid is daarom een belangrijke eigenschap van de FG.

3. Diplomatiek

De FG voert zijn toezicht en controlerende rol op een onafhankelijke wijze uit binnen de gemeente. Hierbij zijn verschillen van inzicht met de verantwoordelijke niet uit te sluiten. Bij het uitoefenen van toezicht op de naleving van de Wbp en sectorspecifieke regelgevingen kunnen bedrijfsbelangen lijken te conflicteren met privacybelangen. Het vergt een zekere behendigheid koers te houden tussen de diverse belangen.
Diplomatieke vaardigheden is daarom een vereiste.

Kerntaken

- Opstellen, uitwerken, implementeren en beheren van het privacy beleid binnen de gemeente.
- Toezicht houden op en controleren van activiteiten binnen de gemeente op het gebied van de organisatorische en technische verwerking van persoonsgegevens.
- Verzamelen van inventarisaties van gegevensverwerkingen.
- Het bijhouden van meldingen van gegevensverwerkingen.
- Rapporteren over privacy aan het College van Burgemeester & Wethouders.
- Het geven van voorlichting en het coördineren en uitvoeren van trainingen binnen de gemeente over privacy gerelateerde onderwerpen.
- Aanspreekpunt voor burgers en medewerkers over privacy vraagstukken, klachten en/of incidenten.
- Adviseren over technologie en beveiliging omtrent de gegevensverwerking.

Vereisten

- Sterke affiniteit met de overheidsector.
- Moet over het juiste ervaringsniveau beschikken om Burgemeester, wethouders en directie te adviseren, enthousiasmeren en te sturen in het privacy onderwerp.
- Sterke functionele management vaardigheden.
- Functionele management vaardigheden om mensen te motiveren zonder gebruik te maken van hiërarchische autoriteit. Aantoonbare vaardigheden in het identificeren, analyseren en kritisch kijken naar probleemsituaties om deze op te lossen.
- Moet in staat zijn om helder en duidelijk te communiceren en complexe situaties zodanig te vertalen naar verschillende doelgroepen.
- Moet kunnen werken in multidisciplinaire teams om de vereiste taken uit te kunnen voeren, zoals sociale hulpverleners, business, IT/Informatie en beveiliging specialisten.
- Minimum van 10 jaar relevante informatie op het gebied van privacy en data bescherming, compliance en of informatie beveiliging in de publieke sector.