Quickscan Privacy

Gemeente Renkum

Naar een *way of life*

Opdrachtgever:
Wendela Verkaik
Arnhem, 13 maart 2017

Ons kenmerk 1016234-002

Quickscan Privacy

Gemeente Renkum

Naar een *way of life*

Opdrachtgever:
Wendela Verkaik
Arnhem, 13 maart 2017

Ons kenmerk 1016234-002

CONCEPT

Contactpersoon:
Janine Steenbergen
+31 6 27 08 55 75
j.steenbergen@kplusv.nl

Inhoud

CONCEPT

Bijlagen

Voorwoord

'Het recht om te bepalen hoe je je presenteert'
'Het recht om vergeten te worden'

Stel je voor, je hebt een slechtere periode in je leven gehad. Toen ging het helemaal niet goed. Je hebt via de gemeenten hulp gezocht en deze ook gekregen. Inmiddels gaat het weer beter en ligt die nare periode gelukkig achter je. Je doet je best die periode te vergeten en weer verder te gaan met je leven.

Hoe zou het verder gaan met je leven je lukken als je wist dat de mensen die je nu ontmoet weten of in hun systemen kunnen opzoeken wat er met jou aan de hand is geweest? Hoe vrij zou je je dan voelen? En hoe zou het hun interactie met jou beïnvloeden? Denk bijvoorbeeld aan een sollicitatiegesprek bij de gemeente, je aanmelding op de voetbalclub of je gesprek bij de bank waar je een lening wilt vragen voor de woning die je wilt kopen.

Gegevens die digitaal bewaard worden geven altijd de mogelijkheid weer ingezien te worden. Ook persoonsgegevens. Het inzien kan per ongeluk gaan, via datalekken, maar ook bewust, bijvoorbeeld uit nieuwsgierigheid. En erger nog, een kwaadwillende kan er zelfs misbruik van maken.

Organisaties die die gegevens van burgers verzamelen hebben kennis en kunnen controle uitoefenen en deze burgers beïnvloeden. Dat geldt dus ook voor gemeenten, zeker nu deze veel taken in het sociaal domein uitvoeren. Overheden werken eraan zorgvuldig met gegevens van burgers om te gaan. De archiefwet verplicht hen wel gegevens jaren te bewaren. Wie weet wat er in de toekomst gebeurt?

Het is van belang dat overheden nu bij het verzamelen van gegevens over burgers zeer terughoudend zijn. Alles wat je nu vastlegt, ligt jaren vast. Privacy begint dan ook bij het niet verzamelen van gegevens; bij dataminimalisatie. Zo borgen we dat burgers zo groot mogelijke kans houden 'vergeten te worden' of 'zich vrij kunnen presenteren'.

Hoe zou jij willen dat de gemeente met jouw gegevens omgaat als jij hulp vroeg?

1 Inleiding

Sinds de drie decentralisaties in het sociaal domein verwerken gemeenten veel meer persoonsgegevens dan daarvoor. De combinatie met nieuws over datalekken roept bij veel gemeenten de vraag op: 'hebben wij onze verantwoordelijkheden met betrekking tot privacy goed ingevuld?' Ook in Renkum heeft het thema privacy de aandacht. Er is een RTA werkgroep ICT en privacy ingesteld vanuit de wens als gemeente de privacy van Renkumse inwoners goed te borgen en de inwoners daar passend over te informeren. In september 2016 heeft de werkgroep haar eindverslag opgeleverd. Op de werkvloer leeft ook de behoefte zorgvuldig invulling te geven aan privacy.

Om inzicht te krijgen in de wijze waarop privacy leeft in de ambtelijke organisatie, of privacy voldoende geborgd is en welke lessen wij moeten trekken uit de realiteit op de werkvloer is een quickscan uitgevoerd.

Dit document bevat de resultaten, conclusies en aanbevelingen van de Quickscan Privacy die is uitgevoerd om een beeld te krijgen aan welke facetten van privacy de gemeente aandacht zou moeten besteden.

CONCEPT

1.1 Uitgangspunten

De bevindingen van de raadswerkgroep vormen de basis voor de onderstaande uitgangspunten van de Renkumse aanpak. Privacy doet zich in zeer veel facetten van de dagelijkse uitvoering van de gemeente voor én vraagt veelvuldig afweging van professionals op de werkvloer.

Principle based

In Renkum vormen privacy principes het uitgangspunt ('principle based'). Dit in tegenstelling tot reguleren en protocolleren als uitgangspunt ('rule based'). Privacy doet zich op te veel terreinen in de gemeentelijke processen voor en vraagt maatwerk afwegingen. Daardoor is het onmogelijk via regulering te werken.

Menselijke kant

Renkum kiest voor een focus op de zachte (menselijke) kant van privacy (de kennis, vaardigheden en gedrag van de werknemers). De visie is: vooral kennis (wat valt onder privacy?) en bewust handelen en verantwoordelijkheid nemen voorkomt privacyschending. Voorbeeld: hoe wegen de consulenten in het sociaal domein de zorgrisico's versus de privacyrisico's? Natuurlijk kan de inrichting van de systemen, de ‘harde kant’ van het privacy vraagstuk, helpen te voorkomen dat er onnodig persoonsgegevens worden verwerkt. Echter, de ICT is in toenemende mate niet door Renkum alleen te bekostigen en de inrichting van systemen wordt in toenemende mate bovenlokaal of door de softwareleverancier bepaald.

Risicogericht

Het is onmogelijk naar 100% veiligheid te streven. Dat zou efficiency en effectiviteit in de weg staan en leidt in de praktijk ook tot het ontwijken van regels in zijn algemeenheid.

Compliance Algemene Verordening Gegevensbescherming

De Wet Bescherming Persoongsgevens (Wbp) wordt momenteel vervangen door Europese regelgeving. Sinds 25 mei 2016 is de Europese algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf 25 mei 2018 wordt op deze verordening gehandhaafd. In tussentijd hebben gemeenten de tijd zich voor te bereiden op deze nieuwe regelgeving. Met de AVG is er nog slechts één privacywet voor de hele Europese Unie (EU). De AVG zorgt onder meer voor een versterking van de privacyrechten van de burger. De gemeente krijgt meer verantwoordelijkheid om de privacywetgeving na te leven en aan te tonen dat zij aan de regelgeving voldoet. Als persoonsgegevens op straat zijn komen te liggen, moet de gemeente kunnen laten zien wat gedaan is om dit te voorkomen. De gemeente moet kunnen aantonen, dat de risico's in kaart zijn gebracht met een privacy impact assessment (PIA), dat de risico's zijn vertaald naar maatregelen en dat gecontroleerd is of de maatregelen nageleefd worden. In feite moet de gemeente dus een managementsysteem voor privacy hebben om dit aantoonbaar te kunnen maken. En tot slot is het aanstellen van een Privacy Officer verplicht. Renkum bereidt zich onder andere via deze quickscan voor op de AVG.

Privacy en informatiebeveiliging

Informatiebeveiliging omvat privacy: het bevat ook de bescherming van andere gegevens dan persoonsgegevens. Informatiebeveiliging is in tegenstelling tot privacy niet wettelijk ingekaderd. Dit is de verklaring waardoor informatiebeveiliging tot nog toe in veel gemeenten in mindere mate is uitgewerkt dan privacy. Privacy heeft, vooral door de drie decentralisaties, in korte tijd in veel gemeenten handen en voeten gekregen. Renkum wil informatiebeveiliging vanuit de samenwerking met Arnhem en Rheden aanpakken. Dat laat onverlet dat deze Renkumse aanpak van privacy Renkum nu een handelingsperspectief biedt. De risicogerichte aanpak laat voldoende ruimte voor aansluiting met het genoemde samenwerkingsverband.

1.2 Quickscan

Voor de AVG moet de gemeente kunnen aantonen dat de risico's in kaart zijn gebracht met een privacy impact assessment (PIA), dat de risico's zijn vertaald naar maatregelen en dat gecontroleerd is of de maatregelen nageleefd worden. Renkum wenst een handzame risicoanalyse die organisatiebreed kan worden ingezet, gericht is op de menskant en richting geeft aan een lerende praktijk. Voor deze specifieke eisen hebben wij geen bestaande risicoanalyse gevonden. De beschikbare analyses kennen een sterk (ICT-) technische insteek, zijn opgezet vanuit risk management expertise en daarmee erg abstract, zijn zeer uitgebreid en lastig hanteerbaar óf richten zich alleen op het sociaal domein. KplusV heeft een hanteerbare scan ontwikkeld die inzetbaar is voor het brede palet aan gemeentelijke taken en verdiept op het sociaal domein.

De Quickscan Privacy is ingevuld op basis van een 10-tal interviews met sleutelpersonen.

1.3 Leeswijzer

Hoofdstuk 2 bevat de resultaten van de Quickscan Privacy. In hoofdstuk 3 zijn de conclusies beschreven die getrokken zijn op basis van de resultaten. En hoofdstuk 4 beschrijft de aanbevelingen voor te nemen maatregelen.

2 Resultaten Quickscan

2.1 Inleiding

De Quickscan bestaat uit zes facetten. De facetten zijn gekozen op basis van onderzoek en analyse van diverse relevante documenten, enerzijds algemeen gericht op privacy bij overheidsorganisaties, anderzijds specifiek op het sociaal domein, omdat zich hier de grootste risico's voor gemeenten bevinden, en tot slot op basis van de keuze om alleen menselijke kant te onderzoeken in de scan. In de bijlage is een overzicht van de gebruikte documentatie opgenomen.

2.2 Verantwoordelijkheid gemeente in relatie tot samenwerkigspartners

Waar gaat dit facet over?

Dit facet gaat over de partijen waarmee de gemeente privacygevoelige persoonsgegevens uitwisselt. Welke samenwerkingsvorm is afgesproken en wat is er specifiek afgesproken over de verwerking van persoonsgegevens? Ook gaat dit facet over het doorleven van hoe ver de verantwoordelijkheid van de gemeente reikt ten opzichte van partijen die gegevens bewerken in opdracht van de gemeente. Is bekend waar partijen hun eigen gegevens opslaan? En wat als dat bij een malafide partij blijkt te zijn in een ver land? Of wat gebeurt er als een partij failliet gaat? Het is relevant dit soort vragen te beantwoorden, want de risico's kunnen in het sociale domein groot zijn voor gemeenten.

Wat zijn de resultaten van de quickscan?

In het fysieke domein en bij burgerzaken kunnen de samenwerkingsverbanden en -vormen waar privacy (eventueel een rol speelt) goed benoemd worden (ODRA, ACV, Stimuleringsfonds vastgoed, burgers die specifieke vragen hebben in het kader van planvorming RO en alle dienstverlening die plaatsvindt op basis van BSN-nummers) en is concreet waarin er risico's zouden kunnen liggen. In het sociale domein is bij de inregeling van het sociaal domein naar aanleiding van de drie decentralisaties goed gekeken naar privacy in contracten en convenanten. In de interviews is regelmatig verwezen naar de betrokkenheid van juridische zaken tijdens de contractering. Inmiddels zijn deze contracten al een paar jaar geleden opgesteld en geven geïnterviewden gaven aan dat 'anderen vermoedelijk wel weten hoe afspraken zijn vastgelegd'. Het is niet altijd helder of contracten en convenanten in het sociaal domein up to date zijn met de laatste inzichten. Over de hele organisatie is niet helder wat afspraken over privacy zijn als partners gaan samenwerken, fuseren of failliet gaan. Ook is niet bepaald of de gemeente in een dergelijke situatie verantwoordelijk is. 'Daar zijn geen afspraken over'.

2.3 Organisatie van de taken binnen de gemeente

Waar gaat dit facet over?

Dit facet gaat over de verdeling van het werk in taken en rollen. Dit is alleen belangrijk voor het sociaal domein, omdat daar bewust spanning en ruimte is vormgegeven tussen de materiewetgeving en de privacywetgeving. De mate van horizontale taakintegratie (werknemers werken voor meer wetten, bijvoorbeeld zowel voor de Wmo als voor de Jeugdwet) of verticale taakintegratie (één werknemer doet meer stappen in het proces er zijn daardoor relatief weinig mensen betrokken bij één casus) brengen meer of minder specifieke privacy risico's met zich mee. Ook gaat dit facet over het belang om consistente samenhangende afspraken te maken over wie welke verantwoordelijkheid of taak heeft in de borging van de privacy van burgers. De Privacy Officer (verplicht voor overheden met de ingang van de AVG) is een logische rol om het stelsel van afspraken vorm te geven en te bewaken.

Wat zijn de resultaten van de quickscan?
In het fysieke domein is één concreet voorbeeld beschikbaar waarbij privacyschending een duidelijk risico is. Het gaat om het cameratoezicht op het ACV-terrein Veentjesbrug. In samenwerking met juridische zaken is uitgewerkt wie welke bevoegdheid en taken heeft in verwerking van de gegevens die met de camera worden verzameld. En in de uitvoering worden deze afspraken strikt nageleefd. Bij Burgerzaken is door wetgeving en jarenlange ervaring voldoende bewustzijn over de regels en risico's bij de verwerking van persoonsgegevens en specifiek BSN-nummers. Omdat de wetgeving niet veranderd is is geen informatie naar voren gekomen die aannemelijk maakt dat bij Burgerzaken nu meer privacyrisico's zijn dan voorheen.
In het sociaal domein ligt dit anders. Renkum heeft per wet gespecialiseerde consulenten die de intake, planvorming en uitvoering doen. Alleen bij multiproblemsituaties vindt integraal overleg plaats met de coaches. Dit is een relatief veilige variant als het gaat om compliance aan de privacywetgeving. Maar natuurlijk moet deze organisatievorm wel beheerd en ontwikkeld worden. De rollen die zorgen voor doorontwikkeling en toezicht en controle op de uitvoering van privacy in de processen zijn niet zo duidelijk belegd. Wie is bijvoorbeeld proceseigenaar van de processen waarin persoonsgegevens verwerkt worden? En welke taken horen daarbij? Dat is niet duidelijk. Het is ook niet helder wie stuurt op ontwikkeling van processen en medewerkers op de wijze die past bij de privacyprincipes en vereisten. Ook is niet afgesproken waar de verantwoordelijkheid ligt om te controleren dat alle professionals de stappen doorlopen conform de afspraken die vanuit het oogpunt van privacy zijn gemaakt (controle op casusniveau ligt bij de kwaliteitsmedewerker). De rol van Privacy Officer is in Renkum nog niet belegd.
Kortom, in het sociaal domein is nog geen sprake van een samenhangende geheel van rollen en afspraken die borgen dat privacy-aspecten goed geborgd blijven in de uitvoering en dat ontwikkeling plaatsvindt.

2.4 Processen

Waar gaat dit facet over?
Het facet processen gaat over hoe de gegevensverwerking in de praktijk plaats vindt: vanuit welke grondhouding wordt gewerkt? Wat zijn huidige afspraken over werkwijzen? Bijvoorbeeld afspraken over triage of de mate waarin privacy gevoelige persoonsgegevens binnen de organisatie gedeeld worden tussen collega's. Ander voorbeeld: de wijze waarop BSN-nummers worden gebruikt op documenten die gedeeld worden binnen de gemeente.

Wat zijn de resultaten van de quickscan?
Privacy lijkt in Renkum te zijn vormgegeven vanuit de regels en de processen van de gemeente: 'de gemeente aan het stuur' of vanuit de wens de zorg of ondersteuning zo goed mogelijk in te richten? Bij het inregelen van privacybescherming wordt minder gedacht vanuit het grondrecht op bescherming van de persoonlijke leefsfeer en de gevolgen die het verwerken van persoonsgegevens nu en in de toekomst kan hebben voor de burger. Maar er wordt gewerkt aan verbetering.
Een voorbeeld is dat in het sociaal domein in het kader van integraal kijken gewerkt wordt met de ZRM matrix. Momenteel wordt deze matrix regelmatig standaard volledig ingevuld in de systemen na een gesprek met de burger. Dit is zeer verklaarbaar, omdat het een nieuwe werkwijze is en de medewerkers zich deze nog eigen moeten maken. Maar hierdoor loopt de gemeente privacy risico's, omdat dan niet (per situatie) uitgelegd kan worden waarom alle aspecten van de matrix zijn vastgelegd in relatie tot het *doel* in die situatie (principes van doelbinding en proportionaliteit). Wel is onlangs door de aanpassing in het (GWS) systeem de mogelijkheid ontstaan om per element informatie vast te leggen. Indien daarmee gewerkt wordt, zal dat de privacyrisico's verminderen. Ook zijn systemen inmiddels zo ingericht om 'dat-' en 'wat-informatie' te scheiden is, zodat niet meer gegevens worden gedeeld dan nodig. Hier wordt in de praktijk al redelijk goed mee gewerkt.

Bij het casusoverleg is het doel te komen tot betere zorg. Privacy is daarin vooral een zaak van (statische) regels, afspraken die eenmaal gemaakt zijn en als randvoorwaarde beschouwd worden. Professionals leggen soms wel en soms niet vast waarom ze welke afwegingen maken met betrekking tot privacy.
Overdracht van privacygevoelig persoonsgegevens van de (zorg)uitvoering naar de administratie is een punt van aandacht. Er is afgesproken welke informatie de administratie minimaal nodig heeft voor bijvoorbeeld facturering. Uit efficiency overwegingen is het beeld dat medewerkers nu meer informatie doorsturen naar de administratie dan verantwoord kan worden op basis van de principes uit de privacywetgeving. Dit is eenmaal afgesproken en geïntegreerd in de standaard werkwijze.
De focus in de processen ligt dus nog sterk op efficiency of op het leveren van goede zorg en ondersteuning. Privacy is duidelijk in dit ontwikkelproces wat ondergeschoven.

2.5 Positie van de burger

Waar gaat dit facet over?
Dit facet gaat over de vraag in hoeverre de rechten van de burgers goed uitgeoefend kunnen worden. Is helder waar de burger terecht kan met vragen, verzoeken over zijn/haar persoonsgegevens en klachten? Kan de burger tijdig (binnen vier weken) zijn of haar dossier inzien, gegevens wijzigen of laten verwijderen? Ook in relatie tot partnerorganisaties met wie gegevens over burgers zijn gedeeld? Dit is belangrijk, niet alleen voor de bescherming van de rechten van de individuele burger, maar zeker ook voor het imago van betrouwbare overheid die zorgvuldig omgaat met persoonsgegevens.

Wat zijn de resultaten van de quickscan?
Een burger die in Renkum dienstverlening vraagt waarbij privacygevoelige persoonsgegevens worden verwerkt krijgt informatie over zijn privacyrechten. Dat is goed geregeld. Als de burger deze rechten daadwerkelijk wil uitoefenen wordt het lastiger. Het is niet helder waar de burger terecht kan, hoe lang het duurt en welke ambtenaar in dit proces welke taak heeft. Op de website van de gemeente is alleen informatie te vinden over het opvragen van persoonsgegevens door derden. Niet door de betrokken burger zelf. Ook op andere wijzen (folders, artikel in plaatselijke krant, e.d.) wordt niet of nauwelijks kenbaar gemaakt hoe de gemeente met privacy omgaat. De gemeente moet binnen 4 weken voldoen aan het verzoek van de burger. Daarbij moet in beeld gebracht kunnen worden aan welke partnerorganisaties gegevens zijn verstrekt.
De geïnterviewden hebben geven aan dat de gemeente vermoedelijk 'met kunst en vliegwerk' de informatie kan leveren aan de burger, maar dat dit niet zeker is.

2.6 Bewustzijn medewerkers

Waar gaat dit facet over?
Privacy is geen onderwerp dat je slechts eenmaal hoeft vast te leggen in regels en dat daarna in de bureaulade kan. Het risico op schending van privacyrechten van burgers kan zich op heel veel manieren voordoen en moet, zeker nu in het sociaal domein, onderwerp zijn in de dagelijkse afwegingen die worden gemaakt. In de uitvoering is steeds de vraag: wat is de juiste balans tussen zorgrisico's en privacyrisico's. Dit vereist continu bewustzijn, een leercultuur, bewust gecreëerde leersituaties en medewerkers die vaardig zijn in het maken van bewuste afwegingen tussen zorgbelangen en privacybelangen.

Wat zijn de resultaten van de quickscan?
Bij Burgerzaken zijn medewerkers zich al jarenlang bewust van de eisen die het verwerken van privacygevoelige persoonsgegevens aan hen stelt. In het fysieke domein vindt het op een dergelijk kleine schaal plaats en is deze situatie met zorg ingeregeld en wordt volgens protocollen

uitgevoerd. Het sociaal domein is door de grote en redelijk recente decentralisaties nog in ontwikkeling. Het is complex samenhangend stelsel van wet- en regelgeving dat op een ander uitgangspunt (zelfredzaamheid en eigen kracht) is gestoeld dan het stelsel van voor 2015. Dit vraagt van om veel verandering in gedrag bij medewerkers. Privacy heeft zeker de aandacht gehad bij het inregelen van het sociaal domein in Renkum. De principes van de privacywetgeving zijn bekend en hebben hun vertaling gekregen in (soms globale) aanpakken en/of inrichting van systemen. Ook is het belang van privacy bekend (men handelt er niet altijd naar). Wat nog mist is het los komen van regels. Hier lijkt nu wat verkrampt aan te worden vastgehouden. Het gaat niet om 'wat mag er vanuit privacy?', maar om 'hoe zorgen we dat we ons bewust blijven van privacyrisico's en dat we voortdurend privacy meenemen in onze afwegingen?'. De verantwoordelijkheid hiervoor kan uitsluitend laag in de organisatie gelegd worden. De consulenten/coaches (en kwaliteitsmedewerkers) moeten zelf de afweging maken. In Renkum sluit dit goed aan bij de sturingsfilosofie waarin minder hiërarchie en meer autonomie bij de professional gelegd wordt.
Voorbeelden: Wmo consulenten en jeugdconsulenten hebben soms dringend behoefte in elkaar dossiers te kijken. Dit kan, mits de gegevensverwerking die dan optreedt, in relatie staat tot het doel en proportioneel is. Hier is nu onvoldoende het gesprek over om tot nieuwe inzichten en bewust handelen te komen. Zo mocht de medewerker Veiligheid lange tijd niet in GWS. Dit omdat ooit is afgesproken dat zij geen recht had op een autorisatie.
Op een aantal vragen kwam geen eenduidig antwoord: wanneer gebruik je (onbeveiligde) mail om persoonsgegevens uit te wisselen? Wanneer kijk je in dossiers waar je geen casushouder van bent? En zijn er afspraken over hoe iedereen elkaar daarop scherp houdt? Er zijn geen noemenswaardige signalen van onzorgvuldig gebruik van gegevensdragers (uitdraaien bij de printer, tablet verloren, etc.). Toch vergt het nog aandacht om privacy op de werkvloer onderdeel te maken van de 'way of life'.

2.7 Dossiervorming

Waar gaat dit facet over?
Juist als privacygevoelige gegevens van burgers in dossiers zijn opgeslagen, is de burger kwetsbaar voor privacyschending. De gegevens kunnen gedeeld worden en per ongeluk of expres openbaar worden. Door de inrichting van dossiers in systemen (autorisaties) kan veel ongewenst delen worden voorkomen (bijvoorbeeld door het scheiden van 'dat' en 'wat' informatie), maar ook de terughoudendheid in vastleggen.
Bewaarplicht van dossiers door (gemeentelijke) overheden is onderhevig aan regelgeving. Toch geldt ook hier dat privacygevoelige persoonsgegevens, zeker de speciale persoonsgegevens over onder andere geloof, geaardheid, gezondheid, e.d., eerder vernietigd mogen worden als in relatie tot het doel er onvoldoende reden is ze te bewaren.

Wat zijn de resultaten van de quickscan?
Met de implementatie van Suite voor GWS is scheiding van 'dat' en 'wat' informatie goed geregeld. Ook de gescheiden dossierdelen met autorisaties voor bepaalde delen bevorderen zorgvuldige verwerking van persoonsgegevens. Verantwoording van keuzes in afwegingen tussen zorgbelang of privacybelang in de dossiers is nog een aandachtspunt. Er is geen eenduidig beeld over hoe dat nu plaatsvindt. En wordt momenteel nog niet echt gestuurd op ontwikkeling van real time verantwoording (gelijk met de beschrijving van de casus vastleggen).
In de dossiers van de periode voor Suite voor GWS nog te veel privacygevoelige persoonsgegevens opgeslagen (meer dan verantwoord kan worden voor het doel).
Over de bewaartermijnen van dossiers en ook welke informatie wel en niet bewaard wordt zijn verschillende beelden. Wel wordt altijd verwezen naar een richtlijn: 7 jaar of 15 jaar.

3 Conclusies

Renkum geeft zich rekenschap van de risico's op het gebied van privacy. Zowel bij burgerzaken, in het fysieke domein als in het sociaal domein zijn in contracten, in de verdeling van taken over functies, in protocollen, processen en systemen privacy aspecten meegenomen en uitgewerkt. Ook in het sociaal domein, waar door de drie decentralisaties grotere risico's zijn, is bewustzijn van het belang van bescherming van persoonsgegevens duidelijk aanwezig. Vanzelfsprekend zijn voornamelijk in het sociaal domein nog aandachtspunten. Deze hebben te maken met het feit dat de gemeente nog volop bezig is de transformatie vorm te geven.

We zetten de conclusies op een rij. Per facet geven we een oordeel. Het oordeel is onderscheiden in drie categorieën: groen, oranje, rood. Groen geeft aan dat het facet voldoende onder controle is en er geen risico's uit de quickscan naar voren zijn gekomen die aandacht verdienen. Oranje geeft aan dat er risico's zijn, die binnen bepaalde termijn opgepakt moeten worden. Het oordeel rood staat voor grote risico's waarvoor het advies geldt om deze met prioriteit uit te werken in passende maatregelen.

Facet	Oordeel	Toelichting
Verantwoordelijk-heid gemeente in relatie tot samenwerkings-partners	**oranje** (sociaal domein)	In het fysieke domein is privacy in beperkte mate een issue. In de casus was helder met welke partners en welke contracten en wie verantwoordelijk was. In het sociaal domein is een grote hoeveelheid samenwerkingspartners waar privacy een issue is. Contracten zijn (destijds) met zorg opgesteld. Er is beperkt zicht of contracten qua privacy (nog wel) de juiste reikwijdte hebben. Ook is niet helder wie zich verantwoordelijk voelt of moet voelen voor de inhoudelijke kwaliteit van de contracten.
Organisatie van privacytaken binnen de gemeente	**groen** (fysiek domein en burgerzaken) **oranje** (sociaal domein)	Taken m.b.t. verwerken van privacygevoelige persoonsgegevens zijn in het fysieke domein en bij burgerzaken helder belegd. Ook in het sociaal domein lijken deze taken op het eerste oog goed geborgd. Bij doorvragen is in het sociaal domein niet helder wie verantwoordelijk is voor processen waarin privacy een rol speelt en wie mag beslissen over wijzigingen daarop. Wie bijvoorbeeld controleert of dossiers conform de privacy afspraken zijn gevuld. Ook is niet helder wie kennisontwikkeling op het gebied van privacy moet stimuleren. Er is nog geen sprake van een systematisch opgebouwd governance systeem rondom privacy-taken.
Processen	**groen** (fysiek domein en burgerzaken) **oranje** (sociaal domein)	In het sociaal domein is het werken volgens standaard processen en het doorontwikkelen van de processen en

CONCEPT

		werkwijzen een aandachtspunt. Renkum is voortdurend bezig te ontwikkelen en verbeteren. Bij de doorontwikkeling lijkt de focus momenteel sterker te liggen op het zorgaspect dan op het privacyaspect. Privacy is wel meegenomen bij het inregelen van de systemen, maar lijkt nu niet de aandacht te krijgen die een goede balans vereist. Zo vereist de AVG dat de gemeente te allen tijde kan verantwoorden waarom welke afwegingen zijn gemaakt. Vastlegging van afwegingen (real time) is momenteel geen standaard onderdeel van de processen.
Positie van de burger	**oranje**	Renkum informeert burgers die gebruik maken van diensten over hun privacyrechten. Burgers die deze rechten willen uitoefenen moeten daar te veel moeite voor doen. Het is niet transparant waar zij terecht kunnen. En bij verzoeken bestaat een redelijk risico dat de gemeente niet tijdig (binnen vier weken) kan voldoen.
Bewustzijn van medewerkers	**groen** (fysiek domein en burgerzaken) **rood / oranje** (sociaal domein)	Medewerkers in het sociaal domein zijn zich zeker bewust van het belang van privacy, maar gaan daar wat krampachtig mee om ('wat mag wel en wat mag niet?'). Het besef dat elke professional voortdurend in elke casus expliciete afwegingen moet maken en ook het privacybewust handelen vraagt aandacht. Net als de vaardigheden om dit te doen. Het goed in balans handelen van de professionals is dé kritische succesfactor voor het beperken van privacy risico's. Het creëren van een dergelijke balans kost (leer)tijd. Om dit goed on de knie te hebben voor 25 mei 2018 is het noodzakelijk hier voortvarend mee aan de slag te gaan.
Dossiervorming	**oranje** / **groen** (sociaal domein)	Privacyrisico's door de wijze van dossiervorming spelen met name in het sociaal domein. De systemen in het sociaal domein raken steeds meer gericht op correcte dossiervorming. Medewerkers leren hoe ze dossiers moeten aanleggen zodat deze voldoen aan zowel de vereisten vanuit privacy als vanuit zorg. Dossiers uit het verleden zijn zeker niet allemaal goed vanuit het oogpunt van privacy (te uitgebreid, geen scheiding 'dat-' en 'wat-informatie').

4 Aanbevelingen

De conclusies uit hoofdstuk 3 geven aanleiding tot de volgende aanbevelingen.

Bewustwording: privacy als 'way of life' (sociaal domein)
Investeer in bewust handelen en voldoende expertise op het gebied van privacy bij medewerkers op de werkvloer. Daarmee kan Renkum risico's in grote mate te beperken. Hier volstaat een cursus of workshop niet. Het gaat om een continu proces waarbij medewerkers periodiek reflecteren op casussen, van elkaar leren en zorgen dat op de praktijk gebaseerde handelingsrichtlijnen ontstaan. Zorg dat professionals tijd en aandacht voor leren en reflecteren kunnen, willen en mogen vrijmaken. Het inrichten van de mogelijkheden hiertoe en de sturing hierop van leidinggevenden is noodzakelijke randvoorwaarde. Zo kan privacy 'de way of life' worden die nodig is om als gemeente te ontwikkelen en om gemaakte keuzes tussen privacywetgeving en materiewetgeving goed te kunnen verantwoorden (vereiste vanuit de AVG).

Real time verantwoording borgen (sociaal domein)
In de AVG heeft de gemeente meer verantwoordelijkheid om aan zelf te kunnen aantonen dat zij aan de regelgeving voldoet. Als persoonsgegevens op straat zijn komen te liggen, moet de gemeente kunnen laten zien wat gedaan is om dit te voorkomen. Dit maakt 'real time' verantwoording van keuzes op de werkvloer noodzakelijk. Stuur en controleer erop dat professionals op de werkvloer systematisch hun afwegingen verantwoorden. Per 25 mei 2018 start de naleving van de AVG. Dan moet dit geregeld zijn. De systemen in Renkum bieden de mogelijkheden. De medewerkers zullen het in de praktijk moeten gaan doen. Het advies is hen daarin te begeleiden en ondersteunen. Dan kan real time verantwoording geborgd worden.

De burger sterker in beeld
Zorgvuldige communicatie met de burger over hoe gemeente Renkum omgaat met zijn/haar persoonsgegevens geeft de burger vertrouwen in de gemeente en in de overheid in het algemeen. Het advies aan Renkum is het de burgers makkelijk te maken. Zorgen dat zij geen drempels ervaren als zij hun rechten willen uitoefenen. Dus geef enerzijds op de juiste plekken informatie aan burgers en bied een heldere plek voor vragen.
Geef daarnaast een effectief en efficiënt proces vorm om te zorgen dat burgers binnen vier weken op verzoek hun gegevens kunnen laten verwijderen, aanpassen of inzien. Monitor specifiek de ervaringen van burgers via de burgertevredenheidspeiling

Samenhangende geheel van rollen en afspraken
Op diverse terreinen is aandacht besteed aan privacy aspecten bij het inrichten van het sociaal domein t.g.v. de decentralisaties. De afspraken zijn gemaakt in het kader van de transitie. Deze ligt inmiddels ruim twee jaar achter ons. Momenteel werkt Renkum volop aan de transformatie. Daarin is aandacht voor doorontwikkeling en het toewerken naar gestandaardiseerde werkwijzen. Privacy moet bij deze doorontwikkeling een nadrukkelijkere plaats krijgen. Daarvoor is de ontwikkeling naar een samenhangend stelsel van rollen en afspraken nodig. Dat is er nog niet in Renkum. Binnen de AVG wordt de verantwoordelijkheid voor het creëren van deze samenhang belegd bij de Privacy Officer. In Renkum is nog geen Privacy Officer aangewezen.

Achterstallig onderhoud checken
De Quickscan geeft het beeld dat de huidige contracten en dossiers van afgelopen jaar niet 'privacy-proof' zijn. Nadat de verantwoordelijkheid voor ontwikkeling en beheer van contracten (op het thema privacy) belegd is en een werkwijze voor dossiervorming is het aan te bevelen een check te doen op achterstallig onderhoud.

Bijlage 1

Overzicht gebruikte documentatie:

- 'Zorgvuldig en bewust. Gegevensverwerking en Privacy in een gedecentraliseerd sociaal domein'. Rapportage van een werkgroep van ministeries en VNG. Mei 2014.
- Kamerbrief 'Zorgvuldig en bewust. Gegevensverwerking en Privacy in een gedecentraliseerd sociaal domein'. Mei 2014.
- 'Gegevensuitwisseling in het jeugddomein'. Handreiking privacy vanuit de inrichtingstypes van het sociaal team. VNG. Juni 2015.
- Vragenlijst PIA. Informatie Beveiligings Dienst. April 2014.
- Implementatieplan Privacy Sociaal Domein. VNG. December 2015.
- Factsheet Triage en Privacy Sociaal Domein. VNG. September 2015.
- Extern onderzoek datalek. Gemeente Amersfoort. Juni 2016.
- 'Nieuwe privacyverordening vereist risicogerichte benadering'. Cap Gemini. 2015.
- Privacy Impact Assessment (PIA) - Introductie, handreiking en vragenlijst. NOREA. November 2015.

CONCEPT

Onze contactgegevens

KplusV

Vestiging Arnhem
Postbus 60055
6800 JB Arnhem
Westervoortsedijk 73
6827 AV Arnhem
T +31 (0)26 355 13 55

Vestiging Amsterdam
Postbus 74744
1070 BS Amsterdam
Science Park 402
1098 XH Amsterdam
T +31 (0)20 669 90 66

E info@kplusv.nl
I www.kplusv.nl

Thema's

Over KplusV

Wie we zijn

Wie betrokken is, wordt betrokken. Dat zien we bij KplusV elke dag. Opdrachtgevers en initiators weten ons te vinden. Voor gedegen adviezen. Voor onze kennis van zowel de publieke sector als het bedrijfsleven. Voor onze ervaring met innovatieve projecten. En voor onze ondernemersmentaliteit. Vaak nemen we zelf het initiatief om partijen bij elkaar te brengen. Want we houden van aanjagen en van resultaat.

Wat we doen

We verbinden mensen en mogelijkheden. Daar zijn we goed in. We laten publieke organisaties en bedrijven excelleren, zodat ze het beste uit zichzelf en elkaar halen. Verbinden als middel, niet als doel. Met als gevolg slimme oplossingen die betekenisvol zijn voor maatschappij en opdrachtgevers.
Je vindt ons overal waar mogelijkheden en ambities bij elkaar komen. Bij de publieke sector die voor maatschappelijke uitdagingen staat. Bij ondernemingen met strategische en operationele vraagstukken. Bij organisaties in transitie.

Hoe we verbinden

In ieder geval altijd informeel en collegiaal. Maar met een enorme drive om projecten te laten slagen. Met inspirerende initiatieven en goede ideeën. Als adviseur, kwartiermaker, programmamanager of gids... Zolang het maar slaagt. We denken, durven en doen. Die houding maakt ons tot een modern, no nonsens kennisbedrijf. Flexibel, innovatief en resultaat-gedreven. Aantoonbaar.

En waarom we dat doen

Onze kracht schuilt in onze aanpak: een stevige mix van bedenken, verbinden en doen. Partijen en middelen succesvol bij elkaar brengen. Liefst in een publiek-privaat ecosysteem. Omdat dat mogelijkheden biedt om structureel en langdurig waarde te creëren die je niet alleen kunt bereiken. Wij werken er al sinds 1984 mee. En onze ambitie is daarin marktleider te blijven. Want zo leveren en ervaren we elke dag de toegevoegde waarde ervan. Bij onze projecten, bij onze opdrachtgevers, in de samenleving en bij onszelf... KplusV initieert, adviseert, verbindt en realiseert. Nu en in de toekomst.