ONDERZOEKSRAPPORT

Privacy van burgers met een hulpvraag

maart 2016

Rekenkamer Amsterdam

ONDERZOEKSRAPPORT

Privacy van burgers met een hulpvraag

maart 2016

Colofon
Rekenkamer Amsterdam
Directeur: dr. Jan de Ridder
Onderzoekers: drs. Marien van Grondelle
drs. Johan de Groot
mr. drs. Arjan Kok RA (projectleider)
Myrte Leenheer
drs. Robin van de Maat
dr. Erik Oppenhuis

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

Op tal van terreinen verzamelt de gemeente veel gegevens van haar burgers. Zo ook binnen het sociaal domein. Met ingang van 1 januari 2015 zijn de gemeenten belast met de uitvoering van de Jeugdwet, de Wet maatschappelijke ondersteuning 2015 (Wmo 2015) en de Participatiewet en gaan daarom meer dan voorheen taken uitvoeren op het gebied van jeugd, zorg en werk. Deze *transitie* wordt ook wel de drie decentralisaties genoemd. Deze decentralisaties hebben plaatsgevonden vanuit de gedachte dat de gemeente de bestuurslaag is die het dichtst bij de burger staat en derhalve het meest geschikt is deze taken uit te voeren. De gemeente is daarmee verantwoordelijk geworden voor alle jeugdhulp, met uitzondering van langdurige zorg voor kinderen.[1] Ook is zij verantwoordelijk geworden voor de ondersteuning bij zelfredzaamheid en participatie, begeleiding en persoonlijke verzorging, beschermd wonen en opvang en cliëntondersteuning en voor de begeleiding en ondersteuning van mensen met een beperkt arbeidsvermogen. [2]

Naast deze transitie is er ook sprake van *transformatie* in de werkwijze van de gemeente. Met regie voor de burger, meer preventie, de inzet van wijkteams en een omslag van 'zorgen voor' naar 'zorgen dat'.[3]

De wetgever heeft veel beslissingsruimte toegekend aan de gemeenten als het gaat om de uitvoering van die taken, zowel op gevalsniveau als op het niveau van regelgeving en beleid. Het uitgangspunt van de wetgevingsoperaties is dat vanuit de gemeente maatwerk (´één gezin, één plan, één regisseur') wordt geleverd voor jeugdzorg, werk en inkomen en zorg aan langdurig zieken en ouderen. Deze taken voert de gemeente uit samen met externe partners, terwijl het college van B en W wel verantwoordelijk blijft voor de uitvoering van de wettelijke taak, waaronder het waarborgen van de privacy van haar burgers.

Om deze taken uit te kunnen voeren legt de gemeente gegevens vast over de burger met een hulpvraag en zijn of haar netwerk. Steeds vaker is het voor de taakvoering nodig om gegevens tussen gemeentelijke organisatieonderdelen en met externe partners uit te wisselen.

Aan deze ontwikkeling zitten twee kanten. Enerzijds biedt het uitwisselen van gegevens kansen om effectief, over de eigen schotten heen, problemen aan te pakken en efficiënt te werken, waarbij de professional zijn taak kan uitvoeren en de burger met een hulpvraag goed geholpen wordt. Anderzijds loopt de gemeente in een

[1] Voor 2015 was de jeugdzorg een verantwoordelijkheid van de provincies, viel de jeugd-GGZ onder de Zorgverzekeringswet en AWBZ en de jeugd-LVB onder de AWBZ.

[2] Deze taken zijn vanuit de AWBZ overgebracht naar de Wet maatschappelijke ondersteuning (Wmo).

[3] Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, 7 november 2014, p 10.

poging de efficiëntie en effectiviteit van haar handelen te vergroten, het risico de privacy van burgers onvoldoende te respecteren en te waarborgen. Met *privacy* bedoelen wij in dit verband het recht van elke burger om voor zichzelf te bepalen welke informatie over hem of haar hoe, wanneer, met wie en in welke mate wordt gecommuniceerd en waarbij minimaal aan de vereisten van de Wet bescherming persoonsgegevens is voldaan. De balans tussen beide, 'een goede taakuitoefening en privacy', zal zorgvuldig afgewogen moeten worden door de gemeente.

Vanaf 2013 is er op landelijk niveau een toenemende aandacht voor deze balans. Zowel door de Inspectie SZW, staatssecretaris SZW, ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de Autoriteit Persoonsgegevens – voorheen het College Bescherming Persoonsgegevens (CBP) , de kinderombudsman en in de media. Vaak gaat de discussie over een efficiënte en effectieve dienstverlening door de overheid en de vraag wat daarvoor aan gegevens nodig is, of deze gegevens wel gedeeld mogen worden en met wie, en of deze gegevens voldoende zijn beveiligd.[4] Daarnaast wordt erop gewezen dat gemeentes zich onvoldoende bewust zijn van privacyregels, gegevens delen en vastleggen in één dossier over de domeinwetten (Jeugdwet, Wmo 2015 en Participatiewet) heen, te ruime autorisaties hebben toegekend, burgers onvoldoende voorlichten over hun rechten en plichten, en niet hebben duidelijk gemaakt wie de verantwoordelijke is voor de gegevensverzekering zodat de burger weet wie zij daarvoor moeten aanspreken en eventueel dagen voor de rechter.[5]

Uit het toenemende aantal raadsvragen van de gemeenteraadsleden van Amsterdam leiden wij af dat het onderwerp steeds meer politieke aandacht krijgt. Deze vragen richten zich op de (waarborging van de) privacy van de burger (met een hulpvraag).[6]

De gevolgen voor de burger van de decentralisaties kunnen ook op het gebied van privacy vergaand zijn. Het onderwerp is daarmee van groot maatschappelijk en politiek belang en was voor de rekenkamer aanleiding dit onderwerp op haar onderzoekagenda te plaatsen. De doorslaggevende factor om een onderzoek naar privacy te starten was de keuze van ons burgerpanel in november 2014. Circa 900 Amsterdammers spraken de voorkeur uit dat de rekenkamer het onderwerp *privacy voor burgers* in 2015 zou onderzoeken.

---

[4] Zie hiervoor uitgebreid Rekenkamer Amsterdam, onderzoeksopzet privacy voor burgers, 29 april 2015, de literatuurlijst in bijlage 3 en bijvoorbeeld de uitzending Hoe gaan gemeenten om met privacy bij de uitvoering van de nieuwe Jeugdwet? van de Demonitor.nl (22 november 2015) .

[5] Zie PrivacyCare, 'Privacy Impact Assessment in verband met gegevensverwerking bij de uitvoering van de Jeugdwet door gemeenten' (rapport in opdracht van de Directie Justitieel Jeugdbeleid), gepubliceerd als bijlage bij Kamerstukken I 2014/15, 33 684, Q en de literatuurlijst in bijlage 3.

[6] Voorbeelden van raadsvragen zijn: Privacy in de Jeugdwet (GroenLinks, 10 september 2014), Waarborgen van de privacy met betrekking tot persoonsgevoelige gegevens die naar aanleiding van de decentralisatie in beheer zijn van de gemeente Amsterdam (D66 en GroenLinks, 24 maart 2015), beveiliging van Suwinet (D66, 2 september 2015), beveiliging van emailverkeer over kinderen (D66, 24 september 2015) en mogelijke schending van privacy van cliënten tijdens keukentafelgesprekken door gemeenten (PvdA, 29 september 2015) en waarborgen van de privacy van burgers in Suwinet (GroenLinks, 22 januari 2016).

1.2 Gegevensverwerking in het sociaal domein

Bij de uitvoering van de taken voor jeugd, zorg en werk verwerkt de gemeente samen met gecontracteerde partijen veel persoonsgegevens. Het begrip *gegevens-verwerking* omvat het gehele proces dat een gegeven doormaakt. Het start met het moment van verzamelen van gegevens waarna deze gegevens worden gebruikt en eventueel gedeeld. Het proces eindigt met het moment van vernietiging van gegevens.[7] Binnen het sociaal domein worden veel gegevens verwerkt en uitgewisseld. De belangrijkste actoren binnen het sociaal domein zijn in paragraaf 1.2.1 beschreven en de geautomatiseerde systemen waarvan ze gebruik maken in1.2.2. De wettelijke taken voor de gemeente zijn per 1 januari 2015 aanzienlijk uitgebreid, dit heeft ook zijn weerslag gehad op het denken over privacy. In paragraaf 1.2.3 gaan wij nader op deze ontwikkeling in.

1.2.1 Complexe samenwerking en gegevensdeling

Binnen Amsterdam worden de taken voor zorg voor jeugd, maatschappelijke ondersteuning en participatie door vier verschillende soorten teams verzorgd:[8]

1. **Ouder- en Kindteams (OKT).** De OKT's bieden hulp rondom opgroeien en opvoeden. Elk team bestaat uit een teamleider en Ouder- en Kindadviseurs. Onder deze hulpverleners zijn professionals als jeugdverpleegkundigen, jeugdartsen, jeugdpsychologen en assistenten. Een teamleider is een ambtenaar. Hulpverleners zijn altijd in dienst van één van de 23 gecontracteerde partijen.[9]
2. **Wijkzorg(netwerk)**. De wijkzorgnetwerken bieden onder meer ambulante zorg en ondersteuning aan ouderen, mensen met beperkingen, chronisch zieken, verstandelijk beperkten en mensen met psychische problemen. De hulpverleners zijn in dienst bij één van de 44 gecontracteerde aanbieders voor ambulante ondersteuning of één van de 30 gecontracteerde aanbieders voor dagbesteding.[10] De kwartiermakers Wijkzorg zijn in dienst van de gemeente.
3. **Samen DOEN (team)**. Bij Samen DOEN bieden multidisciplinair samengestelde teams over de leefdomeinen heen ondersteuning aan huishoudens met en zonder kinderen die niet of verminderd zelfredzaam zijn. De hulpverleners zijn in dienst bij één van de 22 gecontracteerde partijen. De teamleiders en teamassistenten zijn ambtenaar.
4. **Activeringsteam.** De activeringsteams ondersteunen werkzoekenden en mensen met een grote afstand tot de arbeidsmarkt. De teams bestaan voor 100% uit ambtenaren. Er wordt samengewerkt met ketenpartners (vaak zijn dat ook ambtelijke organisaties) en externe partners die op basis van inkoop worden ingehuurd.[11]

---

[7] Kamerstukken II, 1997-1998, 25 892, nr 3(MvT), p.52.

[8] Onderstaande informatie is grotendeels ontleend aan Samenwerkend Toezicht Jeugd/sociaal domein i.o., Calamiteitenonderzoek Amsterdam - Borgen van veiligheid in kwetsbare gezinnen, september 2015.

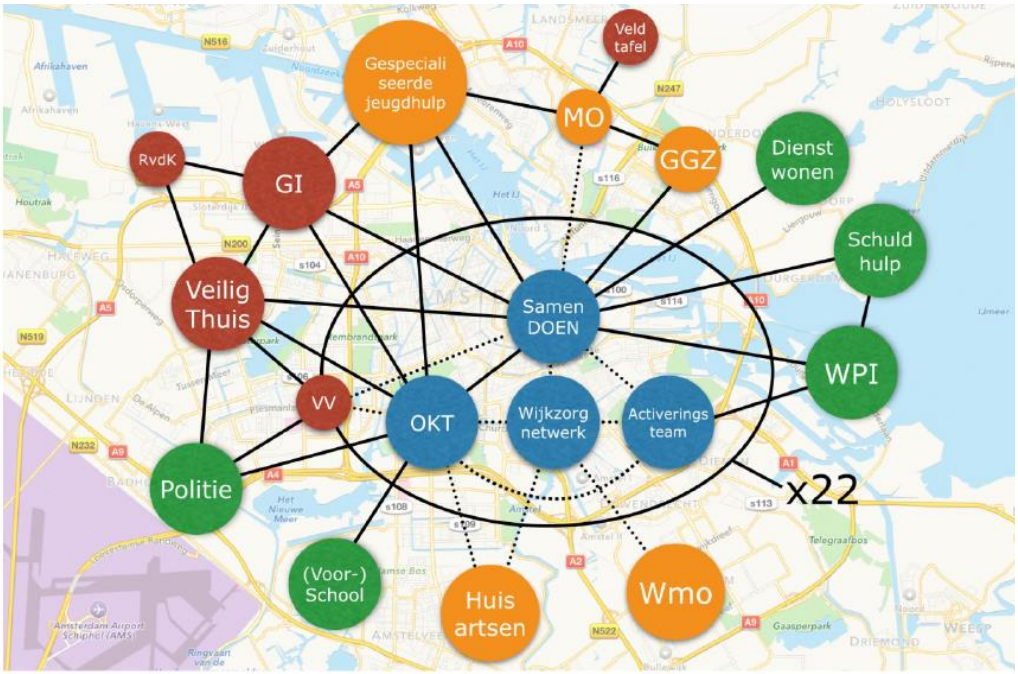
[9] Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014.

[10] Wethouder Zorg en Welzijn, raadsbrief Contractering Wmo 2015, 8 december 2014.

[11] Daarnaast wordt ook samengewerkt met wijkzorg(netwerken).

Amsterdam is voor deze zorg in 22 wijken opgedeeld. In elk van deze wijken is één team van OKT, één team van wijkzorgnetwerk en één team Samen DOEN actief. De zeven activeringsteams bedienen de 22 wijken van de gemeente Amsterdam. De teams kunnen zelf in meer of mindere mate zorg aanbieden of besluiten tot de inzet van gespecialiseerde zorg en ondersteuning.

De teams maken onderdeel uit van een groter netwerk om zorg te verlenen (zie figuur).[12]



Bron: *Calamiteitenonderzoek Amsterdam - Borgen van veiligheid in kwetsbare gezinnen (2015)*

Het figuur laat voor de vier soorten teams zien met wie wordt samengewerkt. Bij deze samenwerking wordt cliëntinformatie uitgewisseld.

De Amsterdamse praktijk is nog complexer omdat de gemeente ook op landelijk en regionaal niveau samenwerkt met zorginstellingen en daarbij zorggerelateerde informatie uitwisselt.[13]

[12] Het samenwerkend toezicht Jeugd/sociaal domein i.o. heeft in september 2015 in kaart gebracht welke partijen betrokken zijn bij de zorg en ondersteuning van kwetsbare gezinnen.

[13] Op landelijk niveau betreft het onder meer de facturering via het Gemeentelijk Gegevensknooppunt (GGK) en berichtenverkeer zorgtoewijzing via het knooppunt VECOSO. Op regionaal niveau worden daarnaast ook berichten uitgewisseld tussen gemeenten en zorgverleners bij het verzoek om toewijzing.

1.2.2 Afzonderlijke registratiesystemen

Voor het vergoeden van de gemaakte zorgkosten en het verantwoordingsproces maakt de gemeente Amsterdam gebruik van WMO-Ned. Dit systeem bevat gegevens over het burgerservicenummer (BSN) gecombineerd met een zorgcategorie van de verleende hulp.

De teams van Samen DOEN, OKT en Wijkzorg werken met het Registratie Informatie Systeem (RIS). RIS bevat zogenaamde 'wat' en 'dat' informatie. 'Dat informatie' heeft betrekking op informatie over het feit dat de burger bekend is bij een instantie en dat aan deze burger hulp wordt of is verleend. De 'wat informatie' betreft zorginhoudelijke informatie en gaat in op de zorgbehoefte van de burger en zijn of haar achtergrond. Op onderdelen kan dit als zeer persoonlijke en gevoelige persoonsgegevens worden ervaren. Een *persoonsgegeven* is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon.[14] Voorbeelden van persoonsgegevens zijn, naam, adres, woonplaats, burgerservicenummer (BSN), maar ook informatie over de dagbesteding, gezinsrelaties en het sociale netwerk van de om hulp vragende burger.[15] Ook worden er *bijzondere persoonsgegevens* geregistreerd.[16] Dit zijn gegevens over de gezondheid en het strafrechtelijke verleden van de betrokkene. De verwerking van deze gegevens is in beginsel verboden behoudens o.a. de noodzakelijke uitvoering van een wettelijke taak of verplichting.

Anders dan de naam doet vermoeden is RIS niet één systeem waarin alle informatie wordt vastgelegd, maar bestaat RIS uit verschillende modules die zijn gekoppeld aan de verschillende soorten wijkteams. Informatieoverdracht van de ene naar de andere module is niet op een geautomatiseerde wijze mogelijk.

In de verschillende modules van RIS wordt persoonlijke informatie vastgelegd over een groot aantal Amsterdammers. Zo heeft OKT over 2015, sinds de start van het programma op 1 januari 2015, 7.288 cliënten geholpen waarvan gegevens zijn vastgelegd in het registratiesysteem RIS.[17] Wijkzorg heeft sinds 1 januari 2015 14.871 dossiers behandeld.[18] Samen DOEN heeft in het jaar 2015 in totaal 3.414 huishoudens weten te bereiken.[19] De activeringsteams maken in zeer beperkte mate gebruik van RIS.[20] Zij gebruiken voornamelijk RAAK (klantmanagement) voor het volgen en registeren van de klant, Focus als paraplusysteem om gegevens uit verschillende

[14] Zie artikel 1 Wbp.

[15] Deze voorbeelden zijn ontleend aan de zelfredzaamheidsmatrix. Voor bijna alle cliënten van wijkzorg en Samen DOEN wordt deze matrix in meer of mindere mate ingevuld wanneer een cliëntdossier wordt aangemaakt.

[16] Zie Paragraaf 2. De verwerking van bijzondere persoonsgegevens van de Wbp.

[17] Mail, 4 februari 2016

[18] Mail, 9 februari 2016; alleen voor burgers met dagbesteding, ambulante ondersteuning en vormen van kortdurende ondersteuning krijgen een dossier in RIS. Andere vormen van Wmo-voorzieningen (zoals vervoersvoorzieningen, trapliften e.d.) worden geregistreerd in Wmo-ned.

[19] Voortgangsrapportage Samen DOEN, januari-december 2015

[20] Een aantal klantmanagers heeft toegang tot RIS om te kunnen raadplegen.

bronnen te raadplegen en Socrates (Inkomen) waarmee de uitkeringen betaald worden.

1.2.3 Groeiende aandacht voor privacy binnen het sociaal domein

Na aanvang van de voorbereidingen in 2014 zijn in 2015 de wijkteams van start gegaan met de nieuwe taken.[21] Niet alleen voor hen was de werkwijze nieuw. Ook voor de ambtelijke organisatie veranderde veel. Naast de nieuwe taken waar de ambtelijke organisatie mee werd geconfronteerd is de ambtelijke organisatie ook gewijzigd als gevolg van een ingrijpende reorganisatie naar clusters en resultaat verantwoordelijke eenheden (RVE's). Het primaire proces - leveren van de zorg - heeft daarbij bestuurlijke en ambtelijke prioriteit gekregen, waarbij er ook aandacht is geweest voor privacy. In de tweede helft van 2015 is de aandacht voor privacy binnen het sociaal domein verder toegenomen. Dit is onder meer af te leiden uit het grote aantal documenten dat vanaf juni 2015 is opgesteld of herzien op dit gebied en de uitgevoerde privacyschouw voor Jeugd (zie paragraaf 3.5.3).

De wijzigingen in het sociaal domein vragen om continue aanpassing van beleid en de werkwijzen van ambtenaren en professionals. Dit was niet alleen tijdens het onderzoek zo, maar deze aanpassingen zullen waarschijnlijk ook in de komende jaren nodig zijn. Wij beschrijven en beoordelen in dit rapport dan ook geen statische situatie maar een veld en werkwijzen die zich continu ontwikkelen in een context van een steeds dynamischer en complexer wordend Amsterdam. Het gaat de rekenkamer er dan ook om inzicht te krijgen in hoe de gemeente omgaat met het vraagstuk van gegevensverwerking en het waarborgen van de privacy van de burgers in het sociaal domein. Enerzijds heeft dit inzicht betrekking op welke afspraken er zijn gemaakt (de *opzet*) en anderzijds hoe deze afspraken in de praktijk worden *uitgevoerd* en worden *ervaren* door ambtenaren en professionals en leden van ons burgerpanel.

1.3 Doelstelling, probleemstelling en onderzoeksvragen

In deze paragraaf behandelen we de doelstelling, probleemstelling, onderzoeksvragen en toetsingskader.

1.3.1 Doelstelling

De rekenkamer beoogt met het onderzoek inzicht te krijgen in de wijze waarop het gemeentebestuur de gegevensverwerking rond twee van de drie decentralisaties – jeugd en zorg- in het sociaal domein heeft geregeld en of daarbij voldoende rekening is gehouden met de privacy van de burgers en of ambtenaren en professionals hun taak kunnen verrichten.

[21] Met uitzondering van de wijkteams Samen DOEN. Deze functioneren al sinds 2012.

Met dit onderzoek willen we een bijdrage leveren aan de verdere ontwikkeling van de dienstverlening aan de burgers, waarbij het recht op bescherming van de privacy wordt gerespecteerd.

1.3.2 Probleemstelling

De centrale vraag van ons onderzoek luidt als volgt:

> Zorgt het college van B en W er voldoende voor dat er zich binnen het sociaal domein een praktijk ontwikkelt waarin een balans wordt gevonden tussen gegevensverwerking en de bescherming van privacy van de burger?

1.3.3 Onderzoeksvragen

Voor de beantwoording van de centrale onderzoeksvraag voor de gemeente Amsterdam hebben we zes onderzoeksvragen beantwoord:[22]

1. Wat wil het college met gegevensverwerking en privacy?
2. Hoe is het organisatorisch geregeld en sluit dit voldoende aan op de Wbp?
3. Hoe worden de organisatorische maatregelen uitgevoerd?
4. Hoe is het proces rondom de cliënt geregeld en sluit dit voldoende aan op de Wbp?
5. Hoe wordt het proces rondom de cliënt uitgevoerd?
6. Wat is balans tussen privacy en gegevensverwerking in de praktijk?

Balans tussen adequate gegevensverwerking en privacy

In onze ogen is van een *adequate gegevensverwerking* sprake wanneer de ambtenaren, hulpverleners en professionals de hen opgedragen taak efficiënt en effectief kunnen uitvoeren met behulp van de verzamelde persoonsgegevens.

Bij het verwerken van persoonsgegevens zullen het gemeentebestuur en de hulpverlenende organisaties een uitdrukkelijke afweging moeten maken tussen het belang van het verwerken van de gegevens en het belang van de *betrokkene* - degene op wie een persoonsgegeven betrekking heeft - om gevrijwaard te blijven van inbreuken op zijn persoonlijke levenssfeer, waaronder zijn privacy.[23] Met *privacy* bedoelen wij in dit verband het recht van elke burger om voor zichzelf te bepalen welke informatie over hem of haar hoe, wanneer, met wie en in welke mate wordt gecommuniceerd en

[22] De onderzoeksopzet van 29 april 2015 bevat drie onderzoeksvragen. Deze onderzoeksvragen zijn tijdens het onderzoek aangepast omdat de visie op de balans tussen gegevensverwerking en privacy in mindere mate aanwezig bleek te zijn in beleidstukken dan wij bij de onderzoeksopzet hadden voorzien. Dit terwijl er binnen de ambtelijke organisatie een toenemende aandacht is voor privacy. Wij hebben daarom de onderzoeksvragen bijgesteld en het accent in aanpak verlegd van onderzoek naar de balans, naar een onderzoek naar de bescherming van privacy.

[23] Zie Ministerie van Justitie, Handleiding voor verwerkers van persoonsgegevens, april 2002, p 25. Uit een toelichting op art 10 van de Grondwet blijkt dat het begrip persoonlijke levenssfeer onder meer betrekking heeft op het huis, de briefwisseling, de communicatie via telefoon en andere communicatiemiddelen, het recht om niet te worden bespied of afgeluisterd, het recht op eerbiediging van het innerlijk leven, het recht op eerbiediging van de lichamelijke integriteit.

waarbij minimaal aan de vereisten van de Wet bescherming persoonsgegevens is voldaan.[24]

In die afweging spelen de gevoeligheid van de te verwerken gegevens en de maatregelen die zijn genomen ter bescherming van de privacy van de betrokkene een rol. [25]

Het vinden van de balans tussen adequate gegevensverwerking en een respectvolle omgang met privacy is niet eenvoudig en wordt vaak beïnvloed door de aard van de problematiek en de fase van gegevensverwerking. In onze onderzoeksopzet hebben wij drie voorbeelden van dilemma's die duidelijk maken hoe complex het maken van afwegingen is in het geval gegevens mogen worden verzameld over een burger, hoe vaak en wanneer een cliënt om toestemming moet worden gevraagd om gegevens te delen, en tot slot onder welke omstandigheden gegevens op verzoek van de burger worden aangepast.[26]

1.3.4 Toetsingskader

De eerste onderzoeksvraag – over wat het college wil met privacy - is beschrijvend van aard. De organisatorische afspraken (onderzoeksvraag 2) toetsen wij aan de hand van vier belangrijke normen afkomstig uit de Wet Bescherming Persoonsgegevens (Wbp). Daarbij gaan wij in op de vraag of deze afspraken er toe bijdragen dat de privacy in *opzet* is geborgd. De *uitvoering* van deze organisatorische afspraken (onderzoeksvraag drie) toetsen wij aan de normen uit de Wbp en aan de normen die de ambtelijke organisatie en de instellingen zich zelf aanvullend hebben opgelegd. Naast de organisatorische afspraken zijn er ook afspraken gemaakt die gericht zijn op de interacties tussen de hulpverlener en ambtenaar enerzijds en de cliënt anderzijds (onderzoeksvraag 4). Deze afspraken brengen in beeld hoe het proces rondom de burger is geregeld. Van deze afspraken toetsen wij of ze in lijn zijn met de Wbp en of ze daarmee de privacy in *opzet* borgen. Hoe deze afspraken in de praktijk uitpakken toetsen wij aan de Wbp en de normen die het ambtelijk apparaat[27] en de instellingen zich zelf aanvullend hebben opgelegd in bijvoorbeeld het privacy protocol (onderzoeksvraag 5). In deze vraag staat daarmee de *uitvoering* centraal. Tot slot is de onderzoeksvraag over de balans tussen gegevensverwerking en privacy (onderzoeksvraag 6) beschrijvend van aard.

[24] Vrij naar de definitie van Westwin zoals opgenomen in Koops en Vedder, Opsporing versus privacy, Universiteit van Tilburg, 2001, p. 16.

[25] Zie Ministerie van Justitie, Handleiding voor verwerkers van persoonsgegevens, april 2002, p 25.

[26] Rekenkamer Amsterdam, onderzoeksopzet privacy voor burgers, 29 april 2015.

[27] Onder het begrip ambtenaren worden ambtenaren verstaan die beleid maken, het beleid uitvoeren, in de backoffice werken ofzorgprofessional of ondersteuner zijn in en van een team of het management vormen van een team.

1.4 Afbakening en aanpak

Het onderzoek richt zich op twee van de drie decentralisaties in het sociaal domein, jeugd en zorg. De Participatiewet hebben wij in dit onderzoek buiten beschouwing gelaten, ondanks dat ook daar het vraagstuk over de balans speelt.

Binnen deze twee domeinen jeugd en zorg hebben wij het onderzoek verder gericht op, Samen DOEN, het Ouder- en Kindteam (OKT), de Wijkzorg en de bijbehorende RIS-modules. Door deze keuzen hebben wij de activeringsteams en de door hen gebruikte systemen, het SUWI-stelsel en het factureringssysteem (WMO-Ned) ook buiten onze onderzoeksscope gelaten. Tevens hebben wij ervoor gekozen om ons onderzoek te richten op de gegevensverwerking en niet specifiek hoe de gegevens worden verkregen – bijvoorbeeld tijdens het keukentafelgesprek – of hoe besluitvorming plaatsvindt op basis van de verkregen gegevens – bijvoorbeeld de indicatiestelling of het besluit tot het toekennen van een persoonsgebonden budget (PGB). Ook hebben we de informatie-uitwisseling op regionaal en landelijk niveau buiten beschouwing gelaten.

De visie op privacy en gegevensverwerking en gemaakte afspraken daarover zijn soms gemeentebreed. Juist daarom hebben wij deze ook in dit onderzoek betrokken.

Voor het beantwoorden van de eerste vier onderzoeksvragen hebben wij gebruik gemaakt van documentenanalyses en interviews. Wij hebben gesproken met onder meer de verantwoordelijke functionarissen en medewerkers van Samen DOEN, OKT en Wijkzorg, het hoofd van de resultaat verantwoordelijke afdeling (rva) Jeugd, de voorzitter en secretaris van Commissie Persoonsgegevens Amsterdam (CPA), medewerkers van CIO-Office en de privacycoördinator van het cluster Sociaal. Bijlage 3 bevat een overzicht van de door ons geraadpleegde functionarissen en documenten.

Voor het beantwoorden van de vijfde onderzoeksvraag - hoe wordt het proces rondom de cliënt uitgevoerd en is dit in lijn met de Wbp en aanvullende regelgeving? - en zesde onderzoeksvraag - wat is de balans tussen privacy en gegevensverwerking in de praktijk? - hebben we gebruik gemaakt van een breedte- en een dieptespoor.

Breedtespoor
In het breedtespoor hebben wij van een aantal van de afspraken voor Samen DOEN, Ouder- en Kindteams en Wijkzorg onderzocht in hoeverre ook uitvoering wordt gegeven aan deze afspraken. Uit overwegingen van eigen doelmatigheid hebben wij een keuze gemaakt in welke afspraken we nader hebben onderzocht.

Wij hebben daarbij gebruik gemaakt van documentanalyses, het internet geraadpleegd, gesprekken gevoerd met leidinggevenden en medewerkers uit de drie verschillende soorten teams en gesproken met de leverancier van RIS. Verder hebben wij gebruik gemaakt van een enquête onder (oud) RIS-gebruikers. In totaal hebben 552 (oud) RIS-gebruikers deze enquête ingevuld. In bijlage 4 is de aanpak van de enquête onder RIS-gebruikers uiteengezet.

Dieptespoor (focusgroep)
Vanwege de meerjarige ervaring met multi-probleemsituaties en het verwerken van (bijzondere) persoonsgegevens hebben wij de Samen DOEN aanpak nader onderzocht. Naast documentanalyses en een gesprek met de programmamanager en medewerkers van Samen DOEN hebben we op 23 november 2015 een groepsgesprek gevoerd met teamleiders, teamassistenten en hulpverleners van Samen DOEN. Deze laatsten zijn werkzaam bij hulpverlenende organisaties waarmee de gemeente een contract heeft afgesloten. Het verslag van dit gesprek hebben wij samengevat in bijlage 6.

1.5 Leeswijzer

Of het college privacybeleid heeft, wat de ambities zijn op het gebied van privacy en wie de verantwoordelijken zijn voor de beleidsvorming en –realisatie, is uiteengezet in hoofdstuk 2. De gemaakte afspraken binnen de gemeente, met samenwerkende instellingen en met de softwareleverancier om de privacy te waarborgen, zijn in hoofdstuk 3 beschreven en beoordeeld. In hoofdstuk 4 is uiteengezet hoe deze afspraken in de praktijk uitpakken. De gemeente heeft met instellingen specifieke en concretere afspraken gemaakt over de te doorlopen stappen bij hulpverlening, de privacyrechten van betrokkenen en voorlichting hierover. Deze afspraken zijn in hoofdstuk 5 getoetst aan de Wet bescherming persoonsgegevens. In hoofdstuk 6 is uiteengezet hoe professionals en ambtenaren deze afspraken ervaren in de praktijk. In hoofdstuk 7 gaan we in op de vraag of de randvoorwaarden op orde zijn om goede belangenafweging tussen privacy en hulpverlening te kunnen maken. In hoofdstuk 8 verleggen we het perspectief naar de burger en kijken we welk beeld het rekenkamerpanel heeft over het opslaan en delen van privacygevoelige gegevens. In hoofdstuk 9 sluiten wij het onderzoeksrapport af met conclusies.

2 Wat wil het college met gegevensverwerking en privacy?

In dit hoofdstuk staat de vraag centraal 'wat het college met gegevensverwerking en privacy wil bereiken'.
De onderzoeksvraag wordt beantwoord aan de hand van de volgende deelvragen:

1. Wat is de visie van het college van B en W? (paragraaf 2.1)
2. Welk beleid en beleidsdoelstellingen heeft het college vastgesteld over gegevensverwerking en privacy? (paragraaf 2.2)
3. Wie zijn verantwoordelijk voor de beleidsvorming en de beleidsuitvoering? (paragraaf 2.3)
4. Hoe is uitvoering gegeven aan deze verantwoordelijkheden? (paragraaf 2.4)

2.1 Visie gegevensverwerking en privacy

In deze paragraaf beschrijven we de visie(s) van het college voor gegevensverwerking en privacy[28]. Wij definiëren in het onderzoek het begrip *visie* als een visionair en ambitieus beeld van wat het gemeentebestuur wil bereiken (voor haar burgers). Het college heeft in 2009 een algemene visie op privacy geformuleerd dat voor het gehele concern van toepassing is. In 2015 heeft zij een specifieke visie vastgesteld die van toepassing is voor de resultaat verantwoordelijke eenheid (rve) jeugd voor de decentralisatie van de jeugdwet.

2.1.1 Algemene visie gegevensverwerking en privacy

Voor de algemene (voor het gehele concern geldende) visie op gegevensverwerking en privacy[29] is *'Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens'* uit 2009 nog steeds het dominante en geldige document voor het integrale privacybeleid voor de gemeente Amsterdam. Deze notitie is niet bestuurlijk vastgesteld als gevolg van de reorganisatie.[30] Volgens de visie in de notitie is het privacybeleid van de gemeente "flankerend beleid met betrekking tot de bedrijfsvoering"[31].

Als hoofdambitie heeft het college voor ICT en de informatievoorziening in dit beleidsdocument het volgende opgenomen: "Informatie van en binnen de Gemeente Amsterdam is volledig, actueel, betrouwbaar, centraal en snel beschikbaar. Het

[28] Zie paragraaf 1.1, Aanleiding en 1.2, Gegevensverwerking in het sociaal domein voor de definities van de begrippen privacy en gegevensverwerking.

[29] Daarvoor hanteren we ook het begrip 'algemeen privacybeleid'.

[30] In de notitie 'Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens' wordt over de notitie vermeld dat deze "destijds niet bestuurlijk is vastgesteld, vanwege de op handen zijnde organisatieverandering." Aanvullend is door de CPA (interview 8 oktober 2015 CPA) aangegeven dat door de instemming van de Stuurgroep IV er gemeentebreed draagvlak was en het beleid kon worden uitgerold. Ook bleek uit een interview van 9 juli met CIO-Office dat dit nog steeds het geldende integrale privacybeleid van de gemeente Amsterdam is.

[31] Bron: Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens, 2009 (blz. 5).

verzamelen (zoeken), verwerken, opslaan en verspreiden van informatie vindt zo efficiënt en zo veilig mogelijk plaats, met inachtneming van de privacywetgeving."[32]

Op basis daarvan heeft het college vijf afgeleide ambities gedefinieerd.
Deze ambities zijn in het kort (1) een informatievoorziening die voldoet aan de burgerservicecode van de gemeente, (2) eenmalige vastlegging en meervoudig gebruik van gegevens, (3) digitaal verzamelen en verwerken van gegevens (4) concernbreed standaardisering van gegevens en (5) professioneel informatie-management. In de visie van het college vormen deze ambities "een uitstekend kader voor de richting van het toekomstige beleid voor het gebruik van persoonsgegevens."[33]

In 2011 motiveert het college waarom de instelling van een Commissie Persoons-gegevens Amsterdam (CPA) binnen het privacybeleid van de gemeente noodzakelijk is. [34] In de visie van het college is voor de gegevensbescherming een commissie beter dan één functionaris omdat in de CPA personen zitten vanuit verschillende disci-plines waardoor breder naar gegevensverwerking en privacy kan worden gekeken. Het college heeft in een aparte notitie[35] de organisatorische inrichting beschreven die voor een goede omgang met persoonsgegevens in de gemeente Amsterdam moet zorgen.

2.1.2 Specifieke visie gegevensverwerking en privacy Jeugdwet

Het college heeft voor de decentralisatie van de Jeugdwet specifiek beleid voor de gegevensverwerking en privacy[36] ontwikkeld. Ook daarin is een visie neergelegd.[37] Het college ziet deze notitie als een "voorbereiding op de privacy in een breder kader, niet alleen voor de jeugd maar voor het gehele sociale domein en bij voorkeur gemeentebreed."[38] Deze bredere visie is nog niet ontwikkeld. [39]

Uit de notie blijkt dat het college vindt dat "het stelsel zodanig ingericht moet zijn dat het voldoet aan de zogenaamde privacy compliance: de gemeente moet inzicht hebben in de verschillende taken en overzicht hebben van de informatiebehoefte per taak. De taken moeten zijn ingericht met een overzicht met de noodzakelijke en wettelijk toegelaten gegevensuitwisseling met betrokken partijen of actoren." [40]

---

[32] Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens, augustus 2009 (blz. 26).

[33] Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens, augustus 2009 (blz. 26).

[34] Nut en noodzaak Commissie Persoonsgegevens Amsterdam, september 2011 (blz. 3).

[35] Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, november 2011.

[36] Daarvoor hanteren we ook het begrip 'specifiek privacybeleid'.

[37] "Wat doet u met mijn gegevens?" Zorg voor de privacy (februari 2015). Dit document is vastgesteld door het college op 3 februari 2015 en ter kennisname aangeboden aan de Raadscommissie voor Onderwijs, Jeugd, Diversiteit en Integratie, Kunst en Cultuur, Lokale Media en Monumenten op 19 maart 2015.

[38] Bron: "Wat doet u met mijn gegevens?" Zorg voor de privacy, februari 2015 (blz. 5).

[39] De decentralisaties 'zorg' en 'participatie'.

[40] Bron: "Wat doet u met mijn gegevens?" Zorg voor de privacy, februari 2015 (blz. 13).

Het college onderstreept dat het hebben van een goed beeld van wat mag en kan met gegevens vertrouwen oplevert bij de burger en de handelingsbekwaamheid bij de uitvoerder vergroot. "Om dit te bereiken is het wenselijk burgers te betrekken bij dit onderwerp en 'open-minded' op te halen hoe vertrouwen over en weer te realiseren is en bij voorkeur niet alleen op het jeugddomein." [41] Later werkt het college in antwoord op de raadsvraag 'Op welke manier privacy van cliënten is gewaarborgd in de jeugdzorg en jeugd GGZ' haar visie nog verder uit en meldt "dat het college van mening is dat er structureel aandacht moet zijn voor privacy. Alleen al omdat het jeugdstelsel zich voortdurend ontwikkelt. En omdat nieuwe risico's om nieuwe maatregelen vragen. De beste borging van de privacy is het niet vastleggen. Dat doen we met zoveel mogelijk gegevens: niet vastleggen als het niet hoeft. Ofwel, we bekijken steeds of de vastgelegde gegevens ook echt nodig zijn. Dit kan in de loop van de tijd ook wel eens veranderen, waardoor we dit niet eenmalig doen, maar met enige regelmaat opnieuw beoordelen."[42]

2.1.3 Conclusie

Er is een concernbrede visie uit 2009 voor gegevensverwerking en privacy beschikbaar. De status van deze visie is niet geheel duidelijk omdat de notitie waarin deze is neergelegd niet is vastgesteld door het college en/of de raad maar door de stuurgroep Informatievoorziening. Volgens de visie dient er samenhang te zijn tussen het privacybeleid en het informatiebeleidsplan omdat privacy nauw gerelateerd is aan het zorgen voor goede informatie en informatiebeveiliging. Informatie moet zo efficiënt en veilig mogelijk worden verwerkt met inachtneming van de privacywetgeving. De concernbrede visie van het college lijkt weinig ambitieus. Het gaat om een goede informatievoorziening die voldoet aan de wet- en regelgeving. De spanning tussen efficiency en privacy komt niet aan bod. Privacybeleid is in de visie van het college flankerend beleid voor de bedrijfsvoering.

Specifiek voor de decentralisatie Jeugdwet is een notitie geschreven waarin ook een visie ten aanzien van privacy en gegevensverwerking wordt verwoord. In die visie klinkt meer ambitie door. Het belang van de burger moet meer centraal staan. Die ambitie blijkt ook uit de beantwoording door het college van raadsvragen in september 2015. Het college stelt daarbij dat er structureel aandacht moet zijn voor privacy vanwege nieuwe risico's die zich aandienen en benadrukt ook dat het principe moet zijn: 'niet vastleggen als het niet hoeft'.

Er is dus een visie, er zijn ambities, maar het college besteedt in zijn visie weinig aandacht aan de balans tussen gegevensverwerking en het waarborgen van privacy voor de burger.

[41] Bron: "Wat doet u met mijn gegevens?" Zorg voor de privacy, februari 2015 (blz. 13).

[42] Beantwoording raadsvragen S. Mbarki en M.F. Poorter door college (nummer 259) 29 september 2015.

2.2 Beleidsdoelstellingen

In deze paragraaf beschrijven we het beleid en de doelstellingen van het college voor gegevensverwerking en privacy zoals deze is opgenomen in de eerder vermelde documenten. Wij definiëren in het onderzoek het begrip *beleid* als het streven naar het bereiken van bepaalde doelen met bepaalde middelen en bepaalde tijdskeuzes.
In de eerste paragraaf zijn de beleidsdoelstellingen van het algemene privacybeleid opgenomen; in de tweede paragraaf de beleidsdoelstellingen van het specifieke privacybeleid voor de jeugdhulp.

2.2.1 Beleidsdoelstellingen algemeen beleid gegevensverwerking en privacy

In 2009 heeft het college de volgende twee doelen voor het privacybeleid geformuleerd[43]:

1. Het beleid voor het gebruik van persoonsgegevens moet primair ondersteunend zijn aan de bestuurlijke wensen voor:

a. betere dienstverlening aan burgers (BurgerServiceCode)
b. betere ketensamenwerking tussen verschillende publieke en private partners en (daaraan gekoppeld) het gebruik van basisregistraties en kernadministraties.

2. De gemeente wil actief beleid voeren om voor burgers inzichtelijk te maken wat de gemeente van burgers weet en om diezelfde burgers hun eigen gegevens te kunnen laten beheren. Dit kan bijvoorbeeld door het gebruik van Persoonlijke Internet Pagina's te bevorderen.

Deze doelen sluiten aan op de visie dat het algemene privacybeleid primair ondersteunend is aan de dienstverlening. Om het beleid te realiseren heeft het college de volgende uitgangspunten geformuleerd:

- De scope van het beleid is het gehele concern, dus inclusief de stadsdelen. Dat wil zeggen dat er op concernniveau:
  a. kaders worden gesteld waarbinnen diensten, bedrijven en stadsdelen invulling geven aan hun verantwoordelijkheid voor het gebruik van persoonsgegevens.
  b. samenwerking tussen diensten, bedrijven en stadsdelen wordt gefaciliteerd en gestimuleerd.
  c. toetsing van het beleid wordt georganiseerd.
- Amsterdam wil dat binnen haar beleid zo min mogelijk eigen regels worden gemaakt en zo veel mogelijk wordt aangesloten bij landelijke standaarden en ontwikkelingen en actief wordt gezocht naar samenwerking (bijvoorbeeld in G4- of VNG-verband).
- Alle communicatie van burgers met de gemeente is voldoende beveiligd in de zin dat de communicatie vertrouwelijk en betrouwbaar is. Persoonsgegevens worden zorgvuldig gearchiveerd.

[43] Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens, augustus 2009 (blz. 7 en 11).

2.2.2 Beleidsdoelstellingen specifiek beleid gegevensverwerking en privacy voor de Jeugdwet

In de notitie ' "Wat doet u met mijn gegevens?" Zorg voor de privacy' verwoordt het college dat zij per 1 januari 2015 verantwoordelijk is voor de uitvoering van de Jeugdwet. De gemeente merkt op dat door de "verschillende decentralisaties zij, meer dan voorheen, persoonsgegevens van haar burgers zal verwerken." Op basis van de notitie kunnen de volgende doelen voor de privacy en gegevensverwerking bij de decentralisatie van de Jeugdwet gedestilleerd worden:

- Doel: "Het verwerken van noodzakelijke informatie over burgers is een middel dat ten dienste staat van de dienstverlening en ondersteuning aan deze burger."

In het landelijke Privacy Impact Assessment Gemeentelijk 3D Informatiehuishouding wordt de gemeenten geadviseerd om overkoepelend privacybeleid te maken, ten minste voor het sociaal domein, omdat dat meer samenhang, eenduidigheid en transparantie brengt voor privacy en het lerend vermogen van de organisatie.[44] Het college heeft echter voor de andere twee decentralisaties en/of het gehele sociaal domein nog geen privacybeleid en -beleidsdoelstellingen ontwikkeld.

2.2.3 Conclusie

Uit de doelstellingen in de beleidsdocumenten blijkt dat het zorgvuldig omgaan met persoonsgegevens gezien wordt als ondersteunend aan de dienstverlening. Zowel het algemene als het specifieke beleid is flankerend beleid met betrekking tot de bedrijfsvoering. Wel wil het college daarbij de positie van de burger in het beheren van hun persoonlijke gegevens versterken. Er is dus aandacht voor het zorgvuldig omgaan met persoonlijke gegevens, maar niet voor de balans tussen gegevensverwerking en het waarborgen van privacy. Privacybescherming krijgt daardoor toch niet de aandacht die het verdient.

We constateren dat het college geen actueel overkoepelend privacybeleid en geen doelstellingen en beleid heeft ontwikkeld voor het sociaal domein als geheel of voor de decentralisaties 'zorg' en 'jeugd' in het bijzonder. Hierdoor kan er gebrek aan samenhang, eenduidigheid en transparantie in het beleid ontstaan en het lerend vermogen van de organisatie verminderen. In het landelijke rapport[45] werd geadviseerd wel beleid en doelstellingen op te stellen.

[44] Privacy Impact Assessment Gemeentelijk 3D Informatiehuishouding, 7 november 2014(blz. 39). Het rapport biedt handvatten om de gemeentelijke organisatie van de gedecentraliseerde taken te toetsen op privacy risico's en waar nodig maatregelen te treffen.

[45] Privacy Impact Assessment Gemeentelijk 3D Informatiehuishouding, 7 november 2014(blz. 39).

2.3 Verantwoordelijken bij beleidsvorming

In deze paragraaf beschrijven we wie er bestuurlijk en wie er ambtelijk verantwoordelijk is voor de beleidsvorming bij het privacybeleid. Dit gebeurt op hoofdlijnen. In hoofdstuk 3 (Hoe is het organisatorisch geregeld) wordt dieper en concreter ingegaan op de verantwoordelijkheden.

2.3.1 Bestuurlijk

De uiteindelijke verantwoordelijkheid voor de beleidsvorming en -uitvoering ligt op bestuurlijk niveau bij het college. Het onderwerp privacy valt – in de scope van dit onderzoek - binnen drie portefeuilles; ICT, Jeugd en Zorg.

Wethouder Duurzaamheid, Openbare Ruimte, Dienstverlening (w.o. ICT) en Bestuurlijk stelsel (wethouder ICT)
In het college is de wethouder ICT verantwoordelijk voor de inhoud van het privacybeleid van het gehele concern. Daarbij passen de volgende verantwoordelijkheden:

- vaststellen van kaderstellende afspraken voor het gebruik van persoonsgegevens;
- zorg dragen voor een organisatie met heldere verantwoordelijkheden voor de betrokken partijen, inclusief een functionerende Commissie Persoonsgegevens Amsterdam (CPA);
- initiëren van ondersteunend concernbeleid om de bescherming van persoonsgegevens te bevorderen.[46]

Wethouder Onderwijs, Jeugd, Diversiteit en stadsdeel Oost (wethouder Jeugd)
De wethouder Jeugd is politiek verantwoordelijk voor specifiek privacybeleid binnen deze portefeuille. Hieronder valt het beleid van OKT en Samen DOEN. De wethouder heeft aangegeven breder aandacht te willen geven aan privacy en dit te betrekken bij de invulling van een mensenrechtenagenda voor de gemeente Amsterdam[47].

Wethouder Zorg en Welzijn, Ouderen, Sport & Recreatie, RO, Grondzaken en stadsdeel Zuid (wethouder Zorg)
Voor de wethouder Zorg geldt ook dat deze politiek verantwoordelijk is voor specifiek (inhoudelijk) privacybeleid dat door de organisaties, die binnen de portefeuille van de wethouder vallen, gemaakt wordt. Hieronder valt ook Wijkzorg.

2.3.2 Ambtelijk

Bij de ambtelijke organisatie is een organisatorisch onderscheid te maken tussen 'algemeen privacybeleid' voor het gehele concern en 'specifiek privacybeleid' dat door een cluster wordt ontwikkeld voor een specifiek domein.

---

[46] Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, september 2011 (blz. 2).

[47] "Wat doet u met mijn gegevens?" Zorg voor de privacy, februari 2015.

Algemeen beleid
De belangrijkste ambtelijke verantwoordelijken bij de algemene beleidsvorming van het privacybeleid zijn CIO-Office en de Chief Information Security Officer functionaris (CISO). Een andere organisatie binnen het stelsel voor privacy is de onafhankelijke Commissie Persoonsgegevens Amsterdam (CPA). Deze heeft adviserend, signalerende en toezichthouden taken ten aanzien van projecten, beleidsvoornemens en vraagstukken met een privacy-component.

CIO-Office
CIO-Office is verantwoordelijk voor het maken van het algemene beleid voor privacy voor het gehele concern en heeft twee taken:
1. In opdracht van de wethouder ICT formuleren en beheren van kaderstellende afspraken voor het gebruik van persoonsgegevens;
2. Het volgen en implementeren van landelijk beleid rond het gebruik van persoonsgegevens.

CIO-Office maakt dus aanvullend beleid. De extra kaders die worden gesteld door CIO-Office ten aanzien van privacy gelden voor het hele concern.[48]

Chief Information Security Officer (CISO)
Binnen CIO-Office is de CISO-functionaris verantwoordelijk voor de invulling van het algemene privacybeleid en de kaderstelling. De CISO van CIO-Office controleert en toetst of het specifiek door een cluster ontwikkeld privacybeleid past binnen het privacybeleid van het concern.

Commissie Persoonsgegevens Amsterdam (CPA)
De CPA[49] is een onafhankelijke commissie die op 8 november 2011 door het college is ingesteld voor het gehele concern.[50] De commissie heeft binnen haar adviserende rol ook als taak, zodra zij dit signaleert, bij het college aan te geven dat voor bepaalde vraagstukken over privacy beleid nodig is.[51]

Cluster specifiek beleid
Naast het algemene privacybeleid dat ontwikkeld wordt voor het gehele concern, kunnen de clusters zelf (specifiek) beleid voor privacy ontwikkelen. Diensten, bedrijven en stadsdelen zijn zelf verantwoordelijk om daarbij binnen het kader van het concernbeleid voor privacy te blijven. De belangrijkste actoren bij het maken van

[48] Interview 9 juli 2015 CIO-Office.
[49] De voorloper van de Commissie Persoonsgegevens Amsterdam (CPA) was de Registratiecommissie. In hetzelfde B&W-besluit heeft het college ingestemd met het voorbereiden van de aanpassing van het raadsbesluit 'Vaststelling Verordening verstrekking persoonsgegevens uit de Gemeentelijke Basisadministratie "zodat de term Registratiecommissie wordt vervangen door de CPA.
[50] Op deze datum is ook het reglement van deze commissie vastgesteld door het college. De CPA heeft een adviserende, controlerende en toezichthoudende rol op het gebied van de bescherming van de persoonlijke levenssfeer (interview 8 oktober CPA).
[51] Interview 8 oktober CPA.

specifiek privacybeleid zijn de directeuren van de clusters, de Privacycoördinator/ Privacy en Informatie Beveiliger (PIB) en de CPA.

Clusters
Binnen de clusters kan domein specifiek beleid ontwikkeld worden. Dit is door de rve onderwijs, jeugd en zorg voor de Jeugdwet gedaan, met de notitie '"Wat doet u met mijn gegevens?" Zorg voor de privacy' .[52]

Privacycoördinator/PIB[53]
De Privacy Informatie Beveiliger (PIB)[54] in de functie van privacycoördinator moet er voor zorgen dat zijn cluster met specifiek privacybeleid voldoet aan de wet en de concernafspraken. Hij kan hierover gevraagd en ongevraagd adviseren.[55]

CPA
CPA heeft tot taak om te adviseren en te toetsen bij de ontwikkeling van specifiek clusterbeleid. Het cluster moet dan een verplichte adviesaanvraag indienen bij de CPA. De CPA is een onafhankelijke partij in het stelsel en kan een andere mening hebben dan het CIO-Office.[56]

2.3.3 Conclusie
De verantwoordelijken en hun rollen bij de beleidsvorming van privacybeleid zijn beschreven. Bestuurlijk is de Wethouder ICT verantwoordelijk voor de inhoud van het privacybeleid van het gehele concern.
Uit de beschrijving van de ambtelijke rollen blijkt een zekere overlap tussen de functies. Zowel de Privacycoördinator, als de CISO en CIO-Office moeten toetsen of het cluster specifieke beleid past binnen de regelgeving en het concernbrede privacy-beleid. De rol van CISO is een verbijzondering van de CIO-rol. Door deze redundantie bij het toetsen kan er onduidelijkheid ontstaan over rolinvulling ten aanzien van taken, afbakening van taken en verantwoordelijkheden. Het risico bestaat dat deze rol niet goed en volledig wordt ingevuld. In hoofdstuk 4, waar we de uitvoering van het beleid in de praktijk bespreken, komen we terug op deze verantwoordelijk-heden en rollen.

---

[52] Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, september 2011 (blz. 3) en interview 9 juli 2015 CIO-Office.
[53] De rekenkamer hanteert beide termen omdat deze functies en de benamingen ervan in de praktijk door elkaar gebruikt worden. Ook bleek in de praktijk het begrip privacycoördinator gebruikt te worden door functionarissen die als aandachtsgebied privacy hadden. Daarnaast worden ook nog andere benamingen uit het IV-functiehuis zoals cluster privacy officer en dedicated privacyofficer, gehanteerd, maar deze hebben een ander takenpakket.
[54] We gebruiken de term privacycoördinator als we de Privacy Informatie Beveiliger bedoelen in zijn functie van privacycoördinator.
[55] Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van personsgegevens, september 2011 (blz. 5).
[56] Interview 8 oktober CPA.

2.4 Verantwoordelijken voor het realiseren van het beleid

In deze paragraaf beschrijven we wie bestuurlijk verantwoordelijk is en de belangrijkste organisaties en functionarissen waar binnen de gemeente de ambtelijke verantwoordelijkheid is neergelegd voor het realiseren van het privacybeleid. In hoofdstuk 3 (Hoe is het organisatorisch geregeld) zal hier dieper op worden ingegaan.

2.4.1 Bestuurlijk

College
De uiteindelijke verantwoordelijkheid van de uitvoering van het privacybeleid ligt op bestuurlijk niveau bij het college.

Wethouder Duurzaamheid, Openbare Ruimte, Dienstverlening (w.o. ICT) en Bestuurlijk stelsel
De wethouder ICT is verantwoordelijk voor de generieke kaderstelling voor de organisatie en implementatie van het privacybeleid binnen het concern van de centrale stad en stadsdelen. [57]

Wethouder Onderwijs, Jeugd, Diversiteit en stadsdeel Oost
De wethouder Jeugd is verantwoordelijk voor de uitvoering van het privacybeleid binnen zijn domein en binnen de concernkaders. Dit kan het uitvoeren van het specifieke privacybeleid voor de jeugd zijn op basis van de notitie ' "Wat doet u met mijn gegevens?"Zorg voor privacy'. Daarbij is de wethouder bestuurlijk verantwoordelijk voor het toepassen van- en het voldoen aan de concernkaders.
De wethouder Jeugd kan ook de wethouder ICT verzoeken om passende technische maatregelen te treffen voor privacy.[58]

Wethouder Zorg en Welzijn, Ouderen, Sport & Recreatie, RO, Grondzaken en stadsdeel Zuid
De wethouder Zorg is verantwoordelijk voor de uitvoering van het privacybeleid binnen zijn domein, binnen de concernkaders. De wethouder is tevens verantwoordelijk voor de uitvoering van specifiek voor zijn domein ontwikkeld privacybeleid.[59] Daarbij is hij verantwoordelijk voor het toepassen van- en het voldoen aan de concernkaders.

[57] Bronnen: Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens, augustus 2009 (blz. 8) en Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, september 2011 (blz. 2).
[58] Bron: Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, september 2011 (blz. 3) en interview 9 november 2015 OJZ.
[59] Bron: Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, september 2011 (blz. 3).

2.4.2 Ambtelijk

CIO-Office

De dienst ICT/CIO-Office heeft de volgende taken: [60]

- via de reguliere Planning & Control-instrumenten toetsen van de naleving van de afspraken door diensten, bedrijven en stadsdelen;
- voeren van het secretariaat van de CPA;
- adviseren van organisatieonderdelen;
- opzetten en onderhouden van een concernopleiding voor lokale functionarissen.

CIO-Office heeft bij de operationele uitwerking door de clusters een controlerende, toetsende en toezichthoudende rol waarbij gekeken wordt of afspraken binnen de kaders van het concern passen. Daarbij wordt de lijn van BIG (VNG) gevolgd; privacy is de verantwoordelijkheid van de lijnorganisatie.[61] De organisatieonderdelen dienen aan CIO-Office te rapporteren als er incidenten met privacy plaatsvinden.

Bij cruciale projecten neemt CIO-Office deel aan het Stedelijk Advies Team (SAT) waarin verschillende disciplines en rollen zijn vertegenwoordigd. CIO-Office heeft daarin een kaderstellende en toetsende rol ten aanzien van de gemeentelijke Informatievoorziening. Privacy is daar een onderdeel van.[62] SAT onderhoudt ook de contacten met de Cluster Advies Teams (zie kopje IVE's) en de Informatievoorzieningseenheden (IVE's) van de verschillende clusters.

CISO

Bij de uitvoering van het beleid heeft de CISO-functionaris de volgende taken[63]:

- Het jaarlijks plannen en doen uitvoeren van audits;
- Het coördineren van activiteiten bij grote incidenten;
- Het onderhouden van contacten met de landelijke partijen op het gebied van informatiebeveiliging, waaronder het NCSC en de VNG;
- Het verzorgen van het secretariaat voor de Commissie Persoonsgegevens Amsterdam, vindt onder functionele aansturing van de voorzitter van de CPA plaats;
- Het onderhouden van contacten met de landelijke partijen op het gebied van privacy, waaronder het CBP;
- Het organiseren van het noodzakelijke overleg met de clusters en de gezamenlijke stadsdelen;

---

[60] Bron: Taken en verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens, september 2011 (blz.23) en interview 9 juli 2015 CIO-Office.

[61] Voor de informatiebeveiliging committeert de gemeente Amsterdam zich aan het gemeentelijk basisnormenkader voor informatiebeveiliging genaamd Baseline Informatiebeveiliging Gemeente (BIG). De BIG is bedoeld om de gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging, een hulpmiddel te geven om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen, de auditlast te verminderen en gemeenten een aantoonbaar betrouwbare partner te laten zijn. In juni 2015 is het implementatieplan BIG door het Gemeentelijk Management Team (GMT) vastgesteld. Hierin zijn de stappen opgenomen die ervoor moeten zorgen dat aan de landelijke beveiligingsnormen wordt voldaan (bron: Interview, 9 juli 2015).

[62] http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/nieuwsbrief/artikelen-nov-2015-0/sa/

[63] Bron: Privacy en informatiebeveiliging (PIB), 25 juni 2014 en interview CISO 14 december 2015.

- Het verzorgen van bestuurlijke contacten en besluitvorming en het leveren van input bij de P&C-documenten (begroting, rekening, viermaandsrapportages, etc.);
- Het (doen) verzorgen van communicatie c.q. campagnes om privacy en informatiebeveiliging (incl. de fysieke en gedragsaspecten ervan) breed onder de aandacht van de Amsterdamse ambtenaren te brengen;
- Het elke vier maanden rapporteren over de stand van zaken rondom de informatiebeveiliging en de privacy, inclusief de afloop en lessen van incidenten.

Om de uitvoering van het beleid goed te kunnen volgen en te kunnen leren van incidenten organiseert de CISO periodiek overleggen met de PIB-coördinatoren van de clusters/stadsdelen en de coördinator van de infrastructuur (dienst ICT) en het vakoverleg Privacy.[64]

Clusters
De operationele uitwerking van het privacybeleid gebeurt bij de vier clusters (deze taak is georganiseerd binnen vijf zogenaamde informatievoorzieningseenheden (IVE).[65] Conform de lijn van BIG is de directeur van het cluster hiervoor verantwoordelijk. Bij de rve's zitten op gevoelige plekken informatie- en privacybeveiligers. Die rapporteren bij incidenten aan de informatiebeveiliger in het cluster. De clusters zijn verantwoordelijk voor een adequate overlegstructuur binnen het cluster. De clusters dienen zorg te dragen voor een professionele aanpak van de bescherming van de persoonlijke levenssfeer.

Privacycoördinator
Eén van de informatie en privacy beveiligers (de PIB-ers) heeft de rol van privacy-coördinator. Deze coördinator ziet binnen de organisatie toe op de implementatie van het beleid en moet daarbij letten op de 'passendheid' van de organisatorische en technische maatregelen' en de onderling samenhang van die maatregelen. Doordat de coördinerende taak door een PIB-er wordt uitgevoerd is deze medewerker in de praktijk tevens verantwoordelijk voor de (logistieke en fysieke) beveiliging.[66] In het kader van het Informatievoorziening (IV) functiehuis is besloten de functie Privacy- en Informatiebeveiliger (PIB) in 2016 op te splitsen in de functies 'privacycoördinator' en 'informatiebeveiliger' (IB'er).[67] Voor beide functies moet een goede bezetting binnen de clusters aanwezig zijn. De privacycoördinator zal een meer juridisch getinte functie zijn en de IB-functie zal veel meer op het ICT-technisch vlak liggen.[68]

---

[64] Het vakoverleg Privacy is de 'opvolger' van het Privacy Platform met dit verschil dat het vakoverleg Privacy een officiële status heeft (interview 14 december 2015 CISO). Deelnemers zijn: Architectuur, Demandmanagement, IV-Beleid, Portfolio management Functioneel Beheer, Informatiebeheer en Leveranciersmanagement. Het doel van deze overleggen is kennisdeling, creëren van een gezamenlijke werkwijze en het organiseren en vooral stimuleren van de samenwerking.

[65] Interview 9 juli 2015 CIO-Office.

[66] Interview 9 november 2015 OJZ.

[67] Bronnen: Interview, 12 december 2015 en document Stadsbrede IV-kaders, De Basis voor de Amsterdamse informatiehuishouding van CIO-Office van 10 maart 2014 . De genoemde functie is in het IV-functiehuis opgenomen als 'dedicated privacyofficer' .

[68] Interview, 12 december 2015.

BasisInformatie (BI)
De eenheid BasisInformatie (BI, voorheen DPG) is door het college aangewezen als stelselbeheerder basis- en kernregistraties. Dat betekent dat de verstrekking van gegevens uit de basisregistraties aan de onderdelen van het concern Amsterdam in beginsel altijd via BI loopt. Bij een verzoek om gegevens heeft BI een adviserende taak bij het gebruik van de gegevens. BI toetst of de verstrekking van de persoonsgegevens conform de wet- en regelgeving is (zoals wet BRP en Wbp, verordening BRP, reglement BRP) en is toegestaan.[69] Bij een voorgenomen verstrekking van persoons-gegevens vraagt BI ook altijd de CPA om advies. Het advies van CPA is zwaarwegend en in de praktijk wordt er nimmer van afgeweken.

Voor zover het persoonsgegevens betreft uit de BRP vindt er jaarlijks een wettelijk voorgeschreven zelfevaluatie plaats waarbij naast de kwaliteit van de gegevens ook wordt getoetst op het voldoen aan de wettelijke voorschriften op het gebied van privacy en informatiebeveiliging.

Juridische werkgroep 3 D's
De juridische werkgroep 3 D's is specifiek ingesteld in 2013 met als opdracht het "dienstoverstijgend" opzetten van "de juridische ondersteuning van de drie decentralisaties binnen het domein Sociaal en Veilig".[70] Deze werkgroep moet zowel over civielrechtelijke, als over bestuursrechtelijke en aanpalende juridische aspecten adviseren. Op al deze gebieden kan privacy een rol spelen. Civielrechtelijke privacy aspecten spelen er bij inkoop en contractbeheer ICT . Bij (privacy)protocollen en verdeling van bevoegdheden komen we de bestuursrechtelijk privacyaspecten tegen en de aanpalende wetgeving in de Wbp. De juridische werkgroep moet, naast andere taken, in ieder geval zorgen voor een juridische uniformering van de regels bij werkprocessen binnen de teams van de drie decentralisaties. Dit geldt voor de inhoudelijke afspraken (via inkoop of een subsidierelatie) maar ook voor de privacyprotocollen. De werkgroep bestaat inmiddels niet meer.

Juridische werkgroep Samen DOEN
Samen DOEN heeft een juridische werkgroep die iedere maand vergadert om privacyvraagstukken die zich in de praktijk voordoen te bespreken en oplossingen hiervoor aan te dragen.[71]
Informatievoorzieningseenheden (IVE)
In het kader van een verdere professionalisering zijn sinds 1 januari 2015 alle Informatievoorzienings- en Informatiebeheermedewerkers van de gemeente ondergebracht bij vijf IVE's. De IVE's zijn er verantwoordelijk voor dat de informatievoorziening binnen hun cluster zo goed mogelijk is ingericht. Eén van de taken van deze IVE's is het onderdeel 'privacy en informatiebeveiliging'. Concreet betekent dit voor dit onderdeel het in beeld brengen van verwerkingen, meldingen aan CBP, toetsen van verwerkingen en beantwoorden vraagstukken over privacy. De IVE-medewerkers werken daarbij nauw samen met de medewerkers van de rve's.

[69] Interview 9 juli 2015 CIO-Office.
[70] Brief opdrachtformulering Juridische ondersteuning 3 D's, 22 oktober 2013.
[71] Interview 26 oktober en 10 november 2015 Samen DOEN.

De IVE's worden indien nodig geadviseerd door de zogeheten Cluster Advies Teams (CAT). In deze teams wordt er vanuit verschillende disciplines, zoals Architectuur, Privacy- en Informatiebeveiliging en ook BI, gekeken naar projecten. Daarbij is er aandacht voor de passendheid van projectdoelen bij het gemeentelijk beleid, de voortgang van een project, en de uitkomsten van het project. Bij dat laatste zal vooral worden nagegaan of er wordt voldaan aan wet- en regelgeving en interne kaders. Een CAT adviseert, houdt een vinger aan de pols en brengt de IVE in stelling om de eigen rol op te pakken.

Commissie Persoonsgegevens Amsterdam (CPA)
De CPA heeft de volgende taken bij de realisatie van het privacybeleid:
- houden van toezicht op diensten, bedrijven en stadsdelen; dit toezicht is bedoeld in de controlerende zin. Organisaties zijn verplicht tot medewerking en de uitkomsten van een controle kunnen aanleiding zijn tot het doen van aanbevelingen;
- adviseren over beleid (aan wethouder ICT);
- adviseren aan diensten, bedrijven en stadsdelen bij complexe (of politiek gevoelige) vragen[72];
- het jaarlijks opstellen van een programma waarin een aantal prioriteiten voor (ongevraagd) advies en toezicht worden opgenomen;
- indien dit nodig wordt geacht, wordt er met het CBP overlegd.

2.4.3 Conclusie

Op papier zijn de verantwoordelijkheden en rollen voor het realiseren van het privacybeleid beschreven. Uit de beschrijving van de verantwoordelijkheden blijkt een zekere overlap tussen de functies, net als we zagen bij de beleidsvorming. De gemeente is voornemens de PIB op te splitsen in een privacycoördinator en informatiebeveiliger. Dit heeft nog niet zijn weg gevonden in geactualiseerd privacybeleid. Hier zullen we in hoofdstuk 4, bij de uitvoering van het beleid in de praktijk, op terugkomen.

2.5 Beleidsvorming en beleidsuitvoering in de praktijk

We onderzochten of het privacybeleid bij de direct betrokkenen bekend is en uitgevoerd wordt. We constateren op basis van interviews dat er in de praktijk veel aandacht is voor privacy maar dat er bij veel actoren onduidelijkheid is over welke beleidsnotitie leidend is voor het privacybeleid van het gehele concern en welke verantwoordelijkheden, rollen en taken er zijn en wie waarvoor verantwoordelijk is. Veel betrokkenen kenden de concernbrede beleidsnotitie voor privacy niet. Degenen die de notitie wel kenden gaven aan dat er conform deze notitie gewerkt wordt.

[72] Volgens de notitie 'Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens (2011)' kan als richtlijn gedacht worden aan: zaken waar het gebruik van persoonsgegevens een belangrijke rol speelt, tot de kern behoren van het gemeentelijk gebruik van persoonsgegevens, meerdere partijen bij betrokken zijn, ketensamenwerking met externe partijen en zaken waarbij onder gemeentelijke verantwoordelijkheid het gebruik van gevoelige informatie gefaciliteerd wordt.

Een van de meest in het oog springende onduidelijkheden is wie of welk organisatieonderdeel de regie heeft, toetst en controleert of de gegevensverwerking binnen de concernkaders en de wet plaatsvindt. Op papier is dit beschreven, maar in de praktijk blijken veel betrokkenen dit niet te weten. Opvallend is dat de beleidsnotitie voor de Jeugdwet volgens de verantwoordelijke wel getoetst is door CIO-Office en de CPA, conform de afspraken zoals deze in het privacybeleid zijn opgenomen. Van deze toetsing is echter niets op papier te vinden.

2.6 Conclusie

Er is een concernbrede notitie met een visie en beleid over privacy uit 2009. De status van deze notitie is niet duidelijk omdat deze notitie niet is vastgesteld door het college en/of de raad maar door de stuurgroep Informatievoorziening. In de visie van het college zoals deze in andere notities en gesprekken met de raad specifiek vorm heeft gekregen, krijgt de balans tussen gegevensverwerking en het waarborgen van privacy geen aandacht.

In de visie van het college is het concernbrede privacybeleid van de gemeente "flankerend beleid met betrekking tot de bedrijfsvoering". Dit blijkt ook uit het onderbrengen van het onderwerp privacy bij de wethouder ICT; het vormt een randvoorwaarde waaraan ten gevolge van de wet- en regelgeving voldaan moet worden. Het college toont weinig ambitie om een efficiënte bedrijfsvoering op een goede manier te verbinden met het waarborgen van privacy. Algemeen gemeentelijk privacybeleid is verouderd en onbekend bij de organisatie.

Op initiatief van het cluster Sociaal is specifiek privacybeleid opgesteld in 2015 voor de Jeugdwet. Daarin toont het college meer ambitie. Men wil de handelingsbekwaamheid van de uitvoerder vergroten en de burger betrekken bij het onderwerp privacy. In een reactie op raadsvragen geeft het college in september 2015 ook aan dat er structureel aandacht moet zijn voor privacy. Het principe 'niet vastleggen als het niet hoeft' moet daarbij leidend zijn.

De beleidsnotitie voor de Jeugdwet is mogelijk conform het concernbrede privacybeleid getoetst door CIO-Office en/of de CPA. Voor het sociaal domein en in het bijzonder voor de twee andere decentralisaties ontbreken beleidsnotities voor de gegevensverwerking en privacy ondanks dat het Rijk adviseerde dit te doen.

Het beleid moet vorm krijgen op basis van de concernbrede notitie. Deze beleidsnotitie is echter bij vele betrokkenen niet bekend. Degene die de notitie wel kennen, zeggen conform deze notitie te werken.

Zowel bij de beleidsvorming als bij de beleidsrealisatie zijn de rollen onduidelijk verdeeld. Op papier zijn er meerdere organisaties en functionarissen, zoals CIO-Office, CPA, CISO en de privacycoördinator die dit dienen uit te voeren. In de praktijk blijken veel betrokkenen niet te weten bij wie ze moeten zijn en wie wat doet.

De integrale beleidsnotitie uit 2009 die op dit moment de basis vormt van de omgang met privacy door de gemeente, kent niet alleen een aantal manco's, maar is zo langzamerhand ook ingehaald door de praktijk waarin men gezocht heeft en zoekt naar oplossingen voor problemen die zich voordoen.

3 Hoe is het organisatorisch geregeld?

In dit hoofdstuk staat de vraag centraal welke afspraken door of namens het college zijn gemaakt om in *opzet* tot een adequate gegevensverwerking en een respectvolle omgang met privacy te komen. Deze onderzoeksvraag is beantwoord aan de hand van de volgende deelvragen:

1. Welke afspraken zijn binnen de organisatie gemaakt over gegevensverwerking en privacy? (paragraaf 3.2)
2. Welke afspraken zijn met samenwerkende organisaties gemaakt over gegevensverwerking en privacy? (paragraaf 3.3)
3. Welke afspraken zijn met de leverancier van de geautomatiseerde systemen gemaakt over gegevensverwerking en privacy? (paragraaf 3.4)
4. Welke afspraken zijn voor een lerende organisatie gemaakt over gegevensverwerking en privacy? (paragraaf 3.5)

Aan het einde van elke paragraaf zijn de gemaakte afspraken geconfronteerd met de normen afkomstig uit de Wet bescherming persoonsgegevens (Wbp). In paragraaf 3.1 zijn deze normen samengevat.

3.1 Normen Wbp in het kort

De Wet bescherming persoonsgegevens (Wbp) bevat normen voor de omgang met persoonsgegevens en bevat tevens rechten voor de betrokkene. Uit de Wbp hebben wij vier belangrijke normen afgeleid: [73]

1. (Bijzondere) persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en verder worden verwerkt. Verwerking vindt plaats op een behoorlijke en zorgvuldige wijze en gegevens worden niet langer bewaard dan nodig voor het doel.
2. Degene van wie (bijzondere) persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze (bijzondere) persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.
3. De verantwoordelijke zorgt ervoor dat de betrokkene kan beschikken over zijn of haar gegevens en de mogelijkheid heeft om gegevens te verbeteren en verwijderen.
4. De gegevensverwerking moet op een passende manier worden beveiligd en geheimgehouden.

Het normenkader is in Bijlage 2 - Normenkader Wet bescherming persoonsgegevens (Wbp) nader uitgewerkt.

[73] Deze tekst is deels ontleend aan https://www.cbpweb.nl/nl/over-privacy/wetten/wet-bescherming-persoonsgegevens

3.2 Afspraken binnen de organisatie

In deze paragraaf zullen we ingaan op de binnengemeentelijke afspraken die zijn gemaakt om in opzet te komen tot een adequate gegevensverwerking en een respectvolle omgang met privacy. Daarbij komt allereerst de rol van de privacy-coördinatoren van de clusters aan de orde. Dit zijn namelijk belangrijke spelers binnen de organisatie. Zij zijn betrokken bij verschillende procedures, afspraken en maatregelen die de gemeente maakt om privacy te borgen. Vervolgens gaan we in op het Project Portfolio Management (PPM)-proces, de Regeling Risicovolle Projecten (RRP), de advisering vanuit de Commissie Persoonsgegevens Amsterdam (CPA) en op de overige maatregelen die zijn genomen op concernniveau zoals: incidenten- en klachtenmeldingen en het meldpunt datalekken.

3.2.1 Privacycoördinatoren

Privacycoördinatoren zijn betrokken bij het maken van binnengemeentelijke afspraken, bij afspraken met samenwerkende partners en met leveranciers van geautomatiseerde systemen. Tevens zijn zij betrokken bij het bevorderen van een lerende organisatie en nemen zij deel aan het Cluster Advies Team (CAT) om binnen het PPM een advies te geven over het continueren van een PPM-proces. Hun taken, bevoegdheden en verantwoordelijkheden laten zich als volgt samenvatten:[74]

- zorg dragen dat de organisatie voldoet aan de wet en de concernafspraken (in het bijzonder de Wbp).[75] De privacycoördinator voert taken zelf uit, of zorgt ervoor dat deze worden uitgevoerd;
- in kaart brengen van verwerkingen met medewerking van het management;
- meldingen aan het College Bescherming Persoonsgegevens (CBP) van meldingsplichtige verwerkingen;
- stimuleren van privacybewustzijn binnen de eigen organisatie;
- optreden als contactpersoon voor de CPA;
- deelnemen Platform Privacycoördinatoren Amsterdam[76];
- gevraagd en ongevraagd adviseren binnen de eigen organisatie;
- zorg dragen voor afstemming met informatiebeveiliging;
- toetsen van verwerkingen van persoonsgegevens binnen de organisatie; de privacycoördinator is verantwoordelijk voor het beantwoorden van vragen op het gebied van privacy die de bedrijfsvoering betreffen.

Bij het borgen van een adequate gegevensverwerking en het op een juiste wijze verwerken van (bijzondere) persoonsgegevens vervullen privacycoördinatoren een centrale rol. Ze geven advies aan het cluster en hebben een monitorende functie. Deze rol is voornamelijk adviserend, wat betekent dat privacycoördinatoren geen

[74] Notitie 'Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens', 9 december 2011.

[75] De privacycoördinatoren van cluster Sociaal moeten ook kennis hebben van de specifieke domeinwetten, zoals de Jeugdwet en de Wmo 2015.

[76] Het vakoverleg Privacy is de 'opvolger' van het Privacy Platform met dit verschil dat het vakoverleg Privacy een officiële status heeft (Bron: Interview, 14 december 2015).

zeggenschap hebben.[77] De uiteindelijke verantwoordelijkheid voor de uitvoering van adviezen ligt in de business zelf. Mocht er een verschil in inzicht zijn tussen de privacycoördinator en de lijnmanager, dan is de mogelijkheid om te escaleren naar de stedelijk directeur van Cluster Sociaal.[78]

3.2.2 Project Portfolio Management

Projecten die binnen de gemeente Amsterdam gestart worden en een ICT- dan wel een InformatieVoorziening (IV) component hebben, dienen een Project Portfolio Management (PPM) proces te doorlopen.[79] Dit geldt ook voor projecten waar de verwerking van (bijzondere) persoonsgegevens mee gemoeid is.

Het doel van het PPM-proces is het geven van inzicht in de lopende ICT- en IV-projecten binnen de organisatie en duidelijkheid te scheppen of de juiste projecten gestart worden die -zo goed mogelijk- bijdragen aan de doelstellingen van de gemeente. De taken zijn daarbij als volgt verdeeld: het Stedelijk Advies Team (SAT) beoordeelt op stedelijk niveau voornamelijk de 'kritische' projecten en houdt contact met Cluster Advies Teams (CAT) en IV-eenheden van de verschillende clusters.[80] De clusters moeten zorgen dat de kwaliteit van de projecten wordt geborgd en toetsen of de projecten conform de regels, de vooraf gestelde termijn (projectvoortgang) en het budget worden opgestart en uitgevoerd.[81] Daarbij kijken de clusters naar of het project en de uitkomsten van het project wel voldoen aan wet- en regelgeving en kaders.

Elke vier maanden wordt op concernniveau gerapporteerd over de overall status van alle ICT-projecten en –in het bijzonder- over de kritische ICT-projecten.[82] Ook heeft CIO-Office een applicatie tot haar beschikking waarin een grote hoeveelheid projectinformatie te vinden is. Denk bijvoorbeeld aan de beoordelingen van de CAT's; CIO-Office kan zien wat er gerapporteerd wordt over het project en wat het oordeel was van het CAT. Met deze informatie kan CIO-Office zelf haar mening geven als zij het niet eens zijn met de beoordeling van de CAT of signaleert dat de adviezen niet opgevolgd worden. In het kader van de 4-maandsrapportages vinden er over de projecten monitorgesprekken plaats tussen het hoofd van CIO-Office, de IV-managers en de stedelijk directeur.[83]

De fases van het PPM-proces

Het PPM-proces kent vier fases; verkenningsfase, definitiefase, realisatiefase en implementatiefase. Bij de eerste twee fases wordt expliciet stilgestaan bij het onderwerp privacy. De fases kennen haar eigen tussenproducten, zoals: een

[77] Interview, 30 november 2015.

[78] Interview, 30 november 2015

[79] http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/project-portfolio/ppm-inhetkort/

[80] http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/nieuwsbrief/artikelen-nov-2015-0/sa/

[81] Interview, 12 december 2015

[82] Interview, 12 december 2015

[83] Interview, 12 december 2015

projectvoorstel, business case, maar ook risicoanalyses m.b.t. privacy en informatiebeveiliging.[84] Het uitvoeren van een risicoanalyse en –indien noodzakelijk- een aanvullende analyse en/of assessment is vast onderdeel van het PPM-proces en hierin komt privacy nadrukkelijk aan de orde. Voor het gebruik van gegevens uit de Basisregistratie Personen (BRP) zijn aanvullende afspraken gemaakt. Het CAT adviseert bij de faseovergangen in het PPM-proces van de projecten binnen het cluster.[85] Momenteel wordt het PPM-proces herzien en, waar nodig, aangepast.

Voordat de gemeente over gaat tot verwerken van persoonsgegevens wordt, conform de richtsnoeren van het CBP, een verkorte en/of uitgebreide risicoanalyse en een Privacy Impact Assessment (PIA) uitgevoerd.[86] Deze instrumenten zijn als tussenproducten opgenomen in het PPM-proces en zijn bedoeld te inventariseren welke mogelijke risico's kunnen leiden tot beveiligings- en/of privacyincidenten. Van deze incidenten worden de gevolgen en de kans dat deze zich voor doen bepaald. Aan de hand van deze informatie worden (beveiligings)maatregelen getroffen. De privacycoördinatoren moeten voor hun cluster erop toezien of de risicoanalyses en assessments worden uitgevoerd en de juiste maatregelen worden geïmplementeerd.[87] Een CAT adviseert en houdt een vinger aan de pols.[88]

Verkorte risicoanalyses informatiebeveiliging en privacy (VRA)
Het uitvoeren van een Verkorte RisicoAnalyse informatiebeveiliging en privacy (VRA) is tijdens de verkenningsfase van het PPM-proces verplicht. De resultaten van de VRA geven de lijn- en procesmanagers inzicht over de beveiligingsrisico's in het proces en laten tegelijkertijd zien of de standaardbeveiligingen (de zogenaamde baseline informatiebeveiliging van de gemeente Amsterdam) voldoende zijn voor het onderzochte proces. Mocht deze niet volstaan, dan moet er in de definitiefase van het project alsnog een uitgebreide risicoanalyse en/of privacy impact analyse (PIA) uitgevoerd worden. De VRA dient ook te worden verzonden aan de secretaris van de CPA die het ter kennisname kan voorleggen in de CPA-vergadering. Daarnaast kan het CBP toetsen of de risicoanalyse is uitgevoerd.[89]

De VRA bestaat uit drie korte vragenlijsten die door de lijn/business dienen te worden ingevuld. Hierbij kan hulp ingeschakeld worden bij de privacycoördinator van het cluster. [90] In de VRA worden vragen gesteld over o.a. het belang van de processen (de mate van schade die kan ontstaan als de betrouwbaarheid niet op orde

[84] http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/project-portfolio/ppm-proces/.
[85] Voor de reorganisatie van de ambtelijke organisatie (januari 2015) werd de beoordeling van projecten gedaan door CIO-Office. Sinds januari 2015 toetst het CAT de projecten binnen het eigen cluster. Hierdoor wordt een deel van de toetsende rol van projecten door CIO-Office overgedragen naar de clusters. Voor de 'kritische' projecten is de CIO-Office nog wel in beeld (als deelnemer van het SAT) en vindt er een toetsing vanuit CIO-Office plaats (Bron: Interview, 12 december 2015).
[86] Implementatieplan Baseline Informatiebeveiliging Gemeenten (BIG), versie 2, 25 juni 2015.
[87] Interview, 12 december 2015.
[88] http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/nieuwsbrief/artikelen-nov-2015-0/sa/.
[89] Implementatieplan Baseline Informatiebeveiliging Gemeenten (BIG), versie 2, 25 juni 2015.
[90] Verkorte Risicoanalyse Informatiebeveiliging en Privacy, versie 1.5, 8 september 2014.

is), vertrouwelijkheid (gevolgen van onbedoelde of ongeautoriseerde verspreiding van gegevens of informatie) en persoonlijke gevolgen van onbedoelde of ongeautoriseerde verspreiding van persoonsgegevens van betrokkene(n). Ook worden algemene vragen gesteld over de doeleinden, doelbinding van de verwerking van persoonsgegevens en of de betrokkenen op de hoogte zijn van de gegevensverwerking. Mocht in deze laatste vragenlijst een vraag met 'ja' beantwoord worden, dan dient de projectverantwoordelijke contact te zoeken met de privacycoordinator over het uitvoeren van een PIA, een eventuele adviesaanvraag bij de CPA of de melding bij het CBP.[91] De uitkomsten van de vragenlijsten kunnen aanleiding geven voor het nemen van beveiligingsmaatregelen. Met behulp van de scores uit de vragenlijst worden maatregelen benoemd die beveiligingsrisico's moeten verkleinen. Het benoemen van organisatorische maatregelen is belegd bij de lijn en kunnen een middel zijn om de hoge risico's te verminderen tot een acceptabel niveau.

Uitgebreide risicoanalyses informatiebeveiliging en privacy (URA)
De Uitgebreide RisicoAnalyse informatiebeveiliging en privacy (URA) wordt in de definitiefase van het PPM-proces uitgevoerd wanneer blijkt dat de maatregelen uit de baseline niet voldoende zijn en de beveiligingseisen boven een bepaalde grens uitstijgen.[92] Dit is in de vorige fase van het PPM bepaald met behulp van de VRA. De VRA wordt als input gebruikt voor de URA. Met de URA wordt met een quick scan in kaart gebracht welke maatregelen getroffen moeten worden om het juiste niveau van beveiliging te realiseren. Het gaat hier om logische en fysieke beveiliging. Een detailoverzicht met maatregelendoelstellingen uit de URA wordt gebruikt om vast te stellen hoe de implementatiefase moet worden georganiseerd. Hierbij kan bijvoorbeeld een keuze gemaakt worden om bepaalde risico's te accepteren gezien de benodigde maatregelen of dat er op centraal niveau maatregelen genomen worden.[93]

Privacy Impact Assessment (PIA)
Een Privacy Impact Assessment (PIA) wordt uitgevoerd tijdens de definitiefase van het PPM-proces bij nieuwe projecten waar persoonsgegevens verwerkt worden.[94] De PIA kan herhaald worden wanneer de omstandigheden veranderen tijdens de looptijd van een project of als er sprake is van grote wijzigingen in een bestaand systeemproces waarbij persoonsgegevens gebruikt worden.[95] Door het afnemen van een PIA worden voor projecten de mogelijke privacyrisico's bij het gebruik van persoonsgegevens van de betrokken personen en organisaties in kaart gebracht. De PIA laat zien wat de kans is dat de privacy van betrokkenen wordt geschaad, wat de gevolgen hiervan zijn en op welke gebieden dit kan gebeuren. De uitkomsten van de PIA kan de organisatie gebruiken om deze risico's vervolgens te vermijden dan wel te verminderen. In de PIA komen de volgende onderwerpen aan de orde: het type project, de gegevens die gebruikt worden, de partijen die betrokken zijn bij de uitvoering van het project, het verzamelen van gegevens, gebruik van de gegevens

[91] Verkorte Risicoanalyse Informatiebeveiliging en Privacy versie 1.5, 8 september 2014.
[92] Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy, versie 1.2, 4 december 2013.
[93] Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy, versie 1.2, 4 december 2013.
[94] Privacy Impact Analyse: Toelichting, versie 0.1, 6 november 2013.
[95] Privacy Impact Analyse: Toelichting, versie 0.1, 6 november 2013.

(inzien door betrokkenen, corrigeren en verwijderen), het bewaren en vernietigen van gegevens en de beveiliging van gegevens.[96] De PIA doet derhalve geen uitspraak over de naleving van maatregelen (compliance).[97]

De belangrijkste doelen die in het format van de PIA daterend uit 2013 benoemd worden zijn:[98]
- Het voorkomen van kostbare aanpassingen in processen, herontwerp van systemen of stopzetten van een project door vroegtijdig inzicht in de belangrijkste risico's;
- het verminderen van de gevolgen van toezicht en handhaving;
- het verbeteren van de kwaliteit van gegevens, dienstverlening, besluitvorming, de haalbaarheid van een project en de communicatie over privacy en de bescherming van persoonsgegevens;
- het verhogen van het privacybewust zijn binnen een organisatie;
- het verstevigen van het vertrouwen bij de betrokkenen in de wijze waarop persoonsgegevens worden verwerkt en de privacy wordt gerespecteerd.

Het gehanteerde format van de PIA dateert uit 2013. De PIA is nog niet aangepast aan de nieuwe wetgeving.[99]

Opstellen transparantiedocument
Voordat persoonsgegevens uit de Basisregistratie personen (BRP) [100] worden verstrekt, voor bijvoorbeeld een (nieuw) project of een onderzoek, wordt een transparantiedocument opgesteld en wordt door de rve BasisInformatie (BI) beoordeeld of het voldoet aan de wet Basisregistratie Personen.[101] In het document is beschreven welke gegevens uit het BRP worden verstrekt, waarvoor ze worden verstrekt (doelbinding), wie er toegang hebben, hoe de autorisaties geregeld zijn en hoe de beveiliging is geregeld. Ook geeft het inzicht of voor de gegevensverwerking een melding is gedaan bij het CBP. De gemeente geeft aan de transparantie-documenten –indien zaken wijzigen- te actualiseren.[102]

3.2.3 Regeling Risicovolle Projecten

De Regeling Risicovolle Projecten (RRP) is in 2008 door het college ingesteld en stelt extra eisen aan de voorbereiding, uitvoering en beheersing van grote risicovolle projecten. De daadwerkelijke aanwijzing dat een project onder de RRP valt is een besluit van het college van B&W. De voorbereiding, waarin nadrukkelijk aandacht moet worden besteed aan het in beeld brengen van de risico's van het project, mondt

[96] Privacy Impact Analyse: Toelichting, versie 0.1, 6 november 2013.
[97] Privacy Impact Analyse: Toelichting, versie 0.1, 6 november 2013.
[98] Privacy Impact Analyse: Toelichting, versie 0.1, 6 november 2013.
[99] ACAM Auditdienst, Rapport privacycontrol 1ste en 2de lijn, 16 februari 2016. Een recente versie van de PIA is te vinden op site van NOREA.
[100] Dit was voorheen het Gemeentelijke basisadministratie persoonsgegevens (GBA).
[101] Interview, 11 juni 2015.
[102] Stedelijk directeur sociaal, Feitelijk wederhoor, 15 februari 2016.

uit in een zogenaamde 'basisrapportage' voor de gemeenteraad op grond waarvan het definitieve besluit om te starten met het project wordt genomen. Tijdens de uitvoering van het project moet er blijvend aandacht zijn voor de ontwikkeling van de risico's. Wijzigingen in het project, zoals aanpassingen van de scope of het risicoprofiel, moeten altijd vooraf worden voorgelegd voor bestuurlijke besluitvorming. Ook moet de gemeenteraad periodiek via voortgangsrapportages over het verloop van het project worden geïnformeerd. Deze rapportages worden door de Bestuursdienst getoetst op volledigheid en specifiek op het nakomen van gemaakte afspraken naar aanleiding van audits. Hiervoor organiseren bestuursadviseurs zich in een integraal Project Advies Team (PAT-team).

De drie decentralisaties vallen, vanwege hun maatschappelijke en financiële omvang, afzonderlijk onder de Regeling Risicovolle Projecten, waardoor er twee keer per jaar risicoanalyses worden uitgevoerd. Vanwege de onderlinge samenhang en afhankelijkheden wordt daarbij ook gekeken naar de verbinding tussen de drie decentralisaties.[103] Het college van B&W heeft op 24 november 2015 besloten de RRP status voor de drie decentralisaties te beëindigen.[104]

3.2.4 Advisering Commissie Persoonsgegevens Amsterdam

Binnen de gemeentelijke organisatie moet bij complexe of politiek gevoelige kwesties waarin het gebruik van persoonsgegevens een rol speelt, advies gevraagd worden bij de CPA.[105] Een adviesvraag kan vanuit verschillende organisatieonderdelen of functionarissen bij de CPA terechtkomen; bijvoorbeeld vanuit de privacycoördinator of de lijnmanager (in zo'n geval moet de privacycoördinator erbij betrokken worden).[106] De adviezen van de CPA worden volgens de ambtelijke secretaris van de CPA direct teruggelegd aan de ambtelijk verantwoordelijke. Ook wordt er gerapporteerd aan het college. Indien de CPA een advies uitbrengt waarbij zij concludeert dat nog niet aan de maatstaven van de Wbp wordt voldaan dan legt de CPA dit eerst terug bij de functionaris die het advies heeft gevraagd. Geeft deze geen opvolging aan het advies, dan kan de CPA escaleren naar de ambtelijk en/of bestuurlijk verantwoordelijke. Hoewel de CPA de rol van toezichthouder toebedeeld heeft gekregen heeft het geen mogelijkheden om bindende adviezen te geven of opvolging met sancties af te dwingen. De afweging of advies wel of niet wordt overgenomen ligt bij het verantwoordelijke management. De ambtelijke organisatie kan afwijken van het advies van de CPA, maar dit moet wel gemotiveerd en gedocumenteerd worden. De CPA heeft vervolgens de mogelijkheid een gesprek met de wethouder aan te vragen. Het is uiteindelijk aan het college om hier een besluit over te nemen.[107]

---

[103] Gemeentelijke begroting 2015.

[104] Gemeente Amsterdam, Beëindiging van de RRP status voor de 3 decentralisaties, 2 december 2015.

[105] Notitie 'Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens', 9 december 2011.

[106] Interview, 8 oktober 2015.

[107] Interview, 8 oktober 2015.

De behandeltermijn in het reglement van de CPA is voor de adviesaanvragen zes weken.[108] Indien de leden van de CPA het niet eens worden over een standpunt, dan neemt de voorzitter de beslissing. Doordat de commissie breed is samengesteld kan zij vanuit verschillende invalshoeken over de privacyvraagstukken adviseren.

Wbp monitor
Voor haar controlefunctie heeft de CPA de Wbp monitor tot haar beschikking. De Wbp monitor heeft een belangrijke functie bij het zicht krijgen op de gegevens-verwerking binnen de organisatie en het signaleren van risico's. De monitor wordt jaarlijks op verzoek van de CPA uitgevoerd door ACAM, met behulp van jaarlijks herziende vragenlijsten. Wanneer uit de monitor verontrustende signalen of privacyrisico's naar boven komen, kan de CPA er voor kiezen dit verder te laten onderzoeken.[109] In de Wbp monitor van 2015 is ook uitgevraagd of de organisatie-onderdelen de adviezen van de CPA hebben opgevolgd.[110]

3.2.5 Meldingen incidenten, datalekken en klachten

Om de privacy op concernniveau te waarborgen en te verbeteren worden incidenten, datalekken en klachten geregistreerd, afgehandeld en benut.

Incidentenmeldingen
Een bevinding uit de nulmeting (augustus 2015) van de privacyschouw Jeugd (zie paragraaf 3.5.3) was dat er geen procedure was voor het melden van privacy-incidenten.[111] De gemeente heeft hierdoor een maatregel in de vorm van een incidentenrapportage geïmplementeerd. Alle medewerkers van de ambtelijke organisatie en van ketenpartners binnen het Jeugdstelsel, waarmee deze afspraak is gemaakt[112], moeten een melding maken van privacy-incidenten[113] Dat kan via een gestandaardiseerd formulier.[114] Doelen van deze maatregel zijn:

- Het actie ondernemen als een ernstig privacy-incident heeft plaatsgevonden dat nadelig is voor een of meerdere burgers, om het nadeel te beperken of elimineren.[115] Dit kunnen acties zijn op het gebied van kennis/gedrag, afspraken en procedures. [116]

---

[108] Interview, 8 oktober 2015.
[109] Interview, 8 oktober 2015.
[110] Wbp monitor 2015, 11 januari 2016
[111] Rapport Nulmeting Privacyschouw Jeugd Amsterdam, september 2015
[112] Het is de verantwoordelijkheid van de gemeenten om het bestaan en verplichte proces van incidentenmelding met de ketenpartners te communiceren en waar nodig in de (formele) afspraken te borgen. Afhankelijk van de rol van de ketenpartner kan dit gebeuren in werkafspraken, opdrachtformulering, protocol(len) of convenant (bron: Proces omgang met incidenten met (mogelijke) gevolgen voor privacy van burgers binnen Jeugdstelsel, versie 1.0).
[113] Een privacy incident wordt door de gemeente gedefinieerd als een incidenteel voorval waarbij de bescherming van de persoonsgegevens of de processen daar omheen in het gedrang is geraakt of waarbij dit risico wordt opgemerkt (bron: Proces omgang met incidenten met (mogelijke) gevolgen- voor privacy van burgers binnen Jeugdstelsel, versie 1.0).
[114] Interview, 9 november 2015.
[115] Meldformulier incident privacy 2015.
[116] Meldformulier incident privacy 2015.

- Het structureel signaleren van kwetsbaarheden met betrekking tot privacy van betrokkenen (cliënten en andere betrokkenen), zodat de gemeente kan zorgen voor voldoende organisatorische en technische maatregelen op dit vlak.[117]
- Het informeren van het bestuur en management over het aantal, aard en ernst van de incidenten.[118]

De dossierhouder privacy Jeugd geeft de melder van het privacy-incident suggesties en tips hoe het de volgende keer anders en veiliger –in overeenstemming met de Wbp- kan worden gehandeld.[119] Het is nadrukkelijk niet de bedoeling individuele functionarissen af te rekenen. Mocht een functionaris onder verantwoordelijkheid van de Gemeente Amsterdam meerdere malen bij privacy-incidenten betrokken zijn, dan kan de dossierhouder met de functionaris in gesprek gaan. Wanneer dit onvoldoende effectief blijkt, dan wordt een gesprek met de functionaris en het verantwoordelijk management georganiseerd. De dossierhouder brengt vervolgens een advies uit naar het verantwoordelijk management.

Meldpunt datalekken
Vanaf 1 januari 2016 is het voor alle Nederlandse organisaties die werken met privacygevoelige informatie wettelijk verplicht datalekken binnen 72 uur na constatering te melden bij de Autoriteit Persoonsgegevens. Ook dienen de betrokken personen, die mogelijk negatieve effecten ondervinden van het datalek, onverwijld op de hoogte te worden gesteld van het desbetreffende lek. Dit geldt dus ook voor de gemeente Amsterdam. [120]

Bij de gemeente Amsterdam is hiervoor onder verantwoordelijkheid van de CIO-Office een centraal meldpunt voor datalekken ingericht. [121] Meldingen komen centraal binnen in een functionele mailbox. Bij een mogelijk datalek dient de verantwoordelijke van het proces direct een melding te maken bij de CISO en te onderzoeken of er daadwerkelijk sprake is van een datalek dat gemeld moet worden bij de Autoriteit Persoonsgegevens.[122] Meldingen worden ook direct doorgezet naar de PIB'ers van de betreffende clusters. [123] Deze PIB'er moet de melding analyseren en zorgen dat acties worden ondernomen die leiden tot een oplossing. De CISO houdt overzicht en zorgt voor periodieke rapportages. In de overleggen tussen de CISO en de PIB'ers wordt stilgestaan bij de meldingen en afhandeling ervan.[124] Bij complexe zaken kan ook juridische expertise worden ingewonnen van Directie Juridische Zaken (DJZ).[125]

---

[117] Proces omgang met incidenten met (mogelijke) gevolgen- voor privacy van burgers binnen Jeugdstelsel, versie 1.0.
[118] Meldformulier incident privacy 2015.
[119] Interview, 9 november 2015.
[120] Brief Inwerkingtreding meldplicht datalekken per 1 januari 2016, 17 december 2015
[121] Mail, 8 januari 2016.
[122] Brief Inwerkingtreding meldplicht datalekken per 1 januari 2016, 17 december 2015.
[123] Mail, 8 januari 2016.
[124] Mail, 8 januari 2016.
[125] Brief Inwerkingtreding meldplicht datalekken per 1 januari 2016, 17 december 2015.

Klachtenmeldingen
Voor de behandeling van klachten van burgers over de ambtelijke organisatie zijn concernbreed afspraken gemaakt. Volgens de klachtenregeling wordt een klacht integraal, uniform en oplossingsgericht afgehandeld, waarbij de verantwoordelijkheid in de lijn van de gemeentelijke organisatie wordt gelegd.[126] De klachtencoördinator bewaakt het klachtproces, adviseert over klachtbehandeling en is het aanspreekpunt voor herkenning en behandeling. Tevens levert de klachtencoördinator informatie ten behoeve van het leren van klachten.[127] In de stedelijke klachtenregeling zijn tien uitgangspunten opgenomen die als basis dienen voor een behoorlijke omgang met klachten.[128]

3.2.6 Concernauditcommissie

De concernauditcommissie (CAC) heeft tot doel om de kwaliteit en de betrouwbaarheid van de gemeentelijke bedrijfsvoering te bevorderen door onderzoek te doen en ambtelijke top te adviseren over verbeteren. In het 4-lines of defence model is CAC daarmee het derde niveau van interne beheersing. De 1ste lijn van interne beheersing vindt plaats bij de rve's en het lijnmanagement. Op basis van een efficiënte inrichting zijn zij zelf verantwoordelijk voor de signalering, monitoring, afweging en beheersing van risico's in de onderliggende processen en systemen binnen de centraal gestelde kaders en richtlijnen. De 2de lijn bestaat uit medewerkers of afdelingen die zich richten op beleid en ondersteuning ten aanzien van de opzet en bestaan van de beheersing. Het uitgangspunt is een effectief werkende 1ste lijn waardoor de 2de lijn een ondersteunende en toetsende rol kan innemen.[129]

De CAC geeft ACAM opdrachten om onderzoeken uit te voeren. In 2015 is opdracht verstrekt om te onderzoeken in hoeverre de 1ste en 2de lijn de privacycontrol waarborgen zodat aan de Wbp wordt voldaan.

3.2.7 Conclusie

De privacycoördinatoren zijn ervoor verantwoordelijk dat de organisatie ten minste voldoet aan de Wbp en de concernafspraken over privacy. De bevoegdheden van de privacycoördinatoren zijn echter niet toereikend om deze verantwoordelijkheid waar te kunnen maken. De privacycoördinatoren kunnen toetsen, adviseren, overleggen en het privacybewustzijn stimuleren. Ze zijn echter niet bevoegd om te beslissen (over een gegevensverwerking). Deze bevoegdheid ligt in de lijn. De uitkomsten van hun toetsingen en adviezen hebben daarmee een vrijblijvend karakter. Er is dus geen borging dat aan de vier afgeleide normen van de Wbp is voldaan.

Nieuwe projecten doorlopen het Project Portfolio Management proces (PPM-proces) waarbij de organisatieonderdelen worden gedwongen om na te denken over privacy- en beveiligingsrisico's. Deze risico's en benodigde beheersmaatregelen worden

[126] Stedelijke Klachtenregeling Uitgangspunten.
[127] Stedelijke Klachtenregeling Uitgangspunten.
[128] Klachtenregeling Gemeente Amsterdam.
[129] Gemeente Amsterdam, Auditketen (controletoren), 7 oktober 2012.

geïnventariseerd met behulp van de verkorte (en uitgebreide) risicoanalyse informatiebeveiliging en privacy en de privacy impact assessment. Het Cluster Advies Team (CAT) beslist aan het eind van elke fase of de volgende fase mag worden gestart. Tevens moet op basis van de verkorte risicoanalyse informatie-beveiliging en privacy advies worden aangevraagd bij de Commissie Persoons-gegevens Amsterdam (CPA). Daardoor is op hoofdlijnen geregeld dat nieuwe gegevensverwerkingen aan de Wbp en de concernafspraken over privacy, moeten worden getoetst. Hierbij maken we wel de kanttekening dat de CPA geen adequate instrumenten heeft om te toetsen dat de organisatie daadwerkelijk de CPA heeft benaderd voor de verplichte advisering. In de Wbp monitor 2015 is er weliswaar gevraagd of opvolging van een deel van de CPA adviezen heeft plaatsgevonden, maar een onafhankelijk onderzoek hiernaar is niet uitgevoerd. Bovendien kan het organisatieonderdeel besluiten om het advies van de CPA niet of gedeeltelijk op te volgen. Ook het PPM-proces verschaft niet direct inzicht in de wijze waarop het bijdraagt aan een goede invulling van de normen conform de Wbp.

De instrumenten die de gemeente gebruikt om risico's in kaart te brengen zijn vooral gericht op nieuwe projecten. Voor bestaande gegevensverwerkingen ontbreekt een adequate structurele periodieke toets of deze in opzet voldoen aan de Wbp en de concernafspraken over privacy. Op initiatief van de lijn kunnen de uitgebreide risicoanalyse (URA) en de Privacy Impact Assessment (PIA) opnieuw worden afgenomen voor bestaande gegevensverwerkingen, maar een periodieke verplichting ontbreekt. Tevens zijn deze instrumenten niet bedoeld om te toetsen of naleving van wet- en regelgeving in de praktijk ('compliance') plaatsvindt. Op dit vlak zijn geen instrumenten beschikbaar en is niet duidelijk hoe het proces van naleving is ingericht. Daarbij is de gehanteerde format voor het afnemen van de PIA gedateerd en is er inmiddels recentere versie beschikbaar.

Incidenteel kunnen afwijkingen van de Wbp en de concernafspraken gesignaleerd worden met de Wbp monitor en door incident- en datalekmeldingen en klachten. De Wbp monitor is echter in opzet vrij beperkt; het kan informatie geven over privacy-risico's, geeft een overzicht van de verwerking van persoonsgegevens binnen de gemeente en in beperkte mate de opvolging van de CPA adviezen. Het geeft geen inzicht in de kwaliteit van de gegevensverwerking. Voor de CPA kan de Wbp monitor aanleiding geven om verder onderzoek te laten doen en een advies uit te brengen. De geregistreerde incidenten, datalekken en klachten kunnen worden benut voor het verder borgen van de privacy.

Positief is dat de concernauditcommissie heeft laten onderzoeken in hoeverre is gewaarborgd dat de gemeente aan de Wbp voldoet.

3.3 Afspraken met samenwerkende organisaties

Het college van B en W is verantwoordelijk voor de uitvoering van de Jeugdwet en Wmo 2015 (verder domeinwetten). Voor het realiseren van deze wettelijke taak werkt de gemeente samen met 119 partijen.[130] Vanuit die verantwoordelijkheid moet het college verantwoording afleggen hoe geregeld is dat de samenwerkende hulpverlenende organisaties voldoen aan de Wbp en daarmee de privacy waarborgen. Dit vereist dat het college afspraken maakt met de hulpverlenende organisatie over de eisen waaraan de gegevensverwerking moet voldoen, opleidingseisen voor het personeel, maar ook hoe de organisatie zich moet verantwoorden en welke controle- en sanctiemogelijkheden het college heeft. Deze afspraken zijn op managementniveau vastgelegd in samenwerkings-, inkoop- en bewerkersovereenkomsten, en op uitvoerend niveau in privacyprotocollen en werkinstructies.

3.3.1 Verantwoordelijke in de zin van de Wbp

Dat het college van B en W is aangewezen als verantwoordelijke voor de uitvoering van de domeinwetten, maakt niet dat zij ook de verantwoordelijke is in de zin van de Wbp. Volgens de Wbp kan er maar één verantwoordelijke zijn voor de gegevensverwerking. Dit kan bijvoorbeeld het college van B en W zijn, een instelling of een samenwerkingsverband. In Amsterdam is gekozen dat de samenwerkende organisaties, inclusief de gemeente, worden aangemerkt als de verantwoordelijke in de zin van de Wbp.[131]

De Autoriteit Persoonsgegevens kan bij misstanden handhavend optreden (met behulp van een boete) richting de verantwoordelijke. Dat betekent in casu het samenwerkingsverband en niet bij de gemeente of de instellingen afzonderlijk. Voor de betrokkene is het van belang om te weten wie de verantwoordelijke is, omdat deze daar ook zijn of haar recht op inzage, correctie etc. moet uitoefenen en eventueel deze partij voor de rechter moet dagen. Wie verantwoordelijk is heeft ook consequenties voor de rechtsgang. Als de verantwoordelijke een bestuursorgaan is, is er sprake van een bestuursrechtelijke rechtsgang (bezwaar en beroep). Als de verantwoordelijke een civielrechtelijke rechtspersoon is, moet er een civielrechtelijke rechtsgang worden gevolgd.[132]

[130] Zie pararaaf 1.2.1 waarbij het aantal gecontracteerde partijen van OKT, Samen DOEN en Wijkzorg zijn gesommeerd.

[131] Privacyprotocol Samen DOEN, Art. 17; Privacyprotocol Ouder- en Kindteams, Art. 17; Privacyprotocol Wijkzorg, Art. 16.

[132] Zie art. 45 en 46 Wbp.

3.3.2 Samenwerkings- inkoop- en bewerkersovereenkomsten

Om de verschillende taken die de gemeente na de decentralisaties op het gebied van zorg, ondersteuning en jeugdhulp heeft gekregen te kunnen uitvoeren, is, is samenwerking nodig met verschillende partners en instellingen.

Voor Samen DOEN zijn met hulpverlenende instellingen samenwerkings- en inkoopovereenkomsten afgesloten. Hierin staat o.a. vermeld dat de hulpverleners dienen te werken volgens de uniforme werkwijze[133] en dat daarbij het privacyprotocol in acht moeten worden genomen.[134] Het privacyprotocol, waar privacyafspraken in zijn opgenomen, wordt als bijlage meegestuurd bij de samenwerkingsovereenkomst.

In de samenwerkings- en inkoopovereenkomsten van OKT is aangegeven dat de gemeente voor 2015 gezamenlijk met de samenwerkende instellingen nadere afspraken maakt over privacy en de werkwijze binnen OKT.[135] De privacy-afspraken zijn naderhand in het privacyprotocol OKT vastgelegd.[136]

Bij Wijkzorg zijn raam- en bewerkersovereenkomsten met de zorgaanbieders afgesloten.[137] In de bewerkersovereenkomst worden afspraken gemaakt over het zorgvuldig omgaan met de persoonsgegevens die noodzakelijk zijn voor de uitvoering van Wijkzorg. Ook zijn bij Wijkzorg nadere afspraken over privacy gemaakt in een privacyprotocol. In de raam- en bewerkersovereenkomsten wordt hier geen verwijzing naar gemaakt.

In de samenwerkingsovereenkomst van Samen DOEN en OKT is opgenomen dat de hulpverlenende instellingen zullen werken met het (voorlopig) registratie informatie-systeem (RIS) voor de verwerking van persoonsgegevens en informatie-uitwisseling zoals reeds wordt gebruikt.[138] Bij Wijkzorg wordt in de raam- en bewerkersovereen-komst geen verwijzing gemaakt naar RIS. In de overeenkomsten zijn geen bepalingen opgenomen die de instellingen verbieden persoonsgegevens te verwerken ter uitvoering van Samen DOEN, OKT en Wijkzorg in andere registratiesystemen dan RIS. In specifieke gevallen zijn daar duidelijke redenen voor. Bij OKT registreren de medewerkers van de GGD gegevens in het systeem Kidos.[139] Er is gekozen om Kidos naast RIS te zetten om zo aan de verplichtingen op grond van de Wet op de Geneeskundige Behandelingsovereenkomst (WGBO) te kunnen voldoen. De

---

[133] Zie Uniforme Werkwijze Samen DOEN in de buurt versie januari 2015 en paragraaf 3.3.4

[134] Samenwerkingsovereenkomst Samen DOEN in de buurt, oktober 2014, Art. 5; Inkoopovereenkomst Samen DOEN, oktober 2014, Art. 9

[135] Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014, Art. 13; Inkoopovereenkomst Ouder- en Kindteams Amsterdam, september 2014, Art. 9

[136] Addendum Privacy 2015/RIS (bijlage van Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014)

[137] Bij Wijkzorg zijn de algemene afspraken vastgelegd in een raamovereenkomst. Deze is enigszins vergelijkbaar met de samenwerkingsovereenkomsten van Samen DOEN en OKT.

[138] Samenwerkingsovereenkomst Samen DOEN in de buurt, oktober 2014, Art. 12; Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014, Art. 13

[139] Kidos is het medische dossier van de Jeugd en Gezin artsen waarin gezondheidsinformatie staat die niet voor anderen toegankelijk is.

teamleden van Wijkzorg registeren alleen het ondersteuningsplan van de cliënten in RIS. Gegevens met betrekking tot de hulp- of zorgverlening leggen zij vast in het systeem van de moederorganisatie.[140]

Voor Wijkzorg is een boeteclausule opgenomen in de raam- en bewerkersovereenkomsten die in werking treedt zodra de contracterende partij niet (tijdig) de verplichtingen in de genoemde overeenkomsten nakomt.[141] In de samenwerkings- en inkoopovereenkomsten van Samen DOEN en OKT is geen sanctie opgenomen voor het niet nakomen van de verplichtingen in de genoemde overeenkomsten. Wel is opgenomen dat een geschil tussen twee of meerdere partijen wordt voorgelegd aan een zogenaamde geschilbeslechtingcommissie, bestaande uit diverse onafhankelijke deskundigen en ingesteld door de betreffende partijen.[142]

Eind 2014 heeft de gemeente regionaal inkoopovereenkomsten afgesloten met 50 jeugdhulpverleningsinstellingen[143] en 167 groepspraktijken en vrijgevestigden voor de 2e lijns zorg.[144] De overeenkomsten bevatten bepalingen over het juist verwerken van persoonsgegevens en uitwisselen van informatie met inachtneming van de Wbp. Deze zijn niet nader uitgewerkt in bijvoorbeeld privacyprotocollen.

3.3.3 Privacyprotocollen

Om de hulpverleners handvaten te geven hoe zij moeten handelen als het gaat om gegevensverwerking en privacy is voor alle aanbieders en professionals die samenwerken binnen Samen DOEN, OKT en Wijkzorg een privacyprotocol opgesteld. De ketenpartners die aan de samenwerking deelnemen stemmen met het protocol in voor zover het werkzaamheden betreft die hun medewerkers uitvoeren voor Samen DOEN, OKT en Wijkzorg.[145] Een spin-off uit de notitie ' "Wat doet u met mijn gegevens?" Zorg voor de privacy' (2015) is dat de privacyprotocollen zijn herzien.[146] De protocollen zijn in intensief overleg met de sectorvertegenwoordiging opgesteld.[147] De protocollen zijn vastgesteld door het managementteam van Onderwijs, Jeugd, Zorg en Diversiteit.[148] De verschillende werkwijzen met betrekking tot privacy zijn zoveel mogelijk uniform gemaakt. De privacyprotocollen van Samen DOEN, OKT en Wijkzorg worden regelmatig (in ieder geval jaarlijks) beschouwd op eventuele noodzakelijke aanpassingen/up-dates.[149]

---

[140] Privacy Impact Assessment; RIS Modules Om het Kind, Samen DOEN en Wijkzorg, 20 augustus 2014.

[141] Raamovereenkomst Wmo 2015, art. 17; Bewerkersovereenkomst in het kader van Wmo 2015, Art. 9

[142] Samenwerkingsovereenkomst Samen DOEN in de buurt, oktober 2014, art. 16-17; Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014, art. 17-18.

[143] Deze 50 partijen zijn onderdeel van de 119 partijen waar de gemeente mee samenwerkt.

[144] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016. Deze aantallen zijn door stedelijk directeur sociaal aan de Rekenkamer medegedeeld. De Rekenkamer heeft niet de inkoopovereenkomsten met deze partijen in bezit

[145] Privacyprotocol Samen DOEN, Wijkzorg en OKT, preambule.

[146] Interview, 9 november 2015.

[147] Beantwoording raadsvragen Poorter en Mbarki, 29 september 2015.

[148] Interview, 9 november 2015.

[149] Mail, 11 mei 2015 en Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.

In de privacyprotocollen zijn de rechten en plichten van alle betrokkenen van Samen DOEN, OKT en Wijkzorg uitgewerkt en is beschreven tot welke partij de betrokkenen zich kunnen wenden voor het uitvoeren van rechten (e.g. recht op inzage en correctie). Daar waar derden betrokken zijn, wordt beschreven welke bevoegdheden en mogelijkheden zij hebben. Ook zijn de doelen, mate, en de wijze van gegevens-verzameling opgenomen en wordt de lezer geïnformeerd over de bewaartermijn (15 jaar) en geheimhouding bij de gegevensverzameling. Geheimhouding wordt geborgd door de functionarissen die betrokken zijn bij de gegevensverwerking een geheimhoudingsverklaring te laten tekenen en door gebruik te maken van autorisaties in RIS.

De privacyprotocollen geven een opsomming van de (bijzondere) persoonsgegevens die binnen Samen DOEN, OKT en Wijkzorg worden verwerkt. Daarnaast worden voor de hulpverleners regels beschreven die hij/zij in acht moet nemen bij de dossiervorming van cliënten en andere betrokkenen zoals: zo feitelijk mogelijk vastleggen, bronvermelding bij rapporten van externe deskundigen, opschonen persoonlijke werkaantekeningen.

Bij nadere lezing van de privacyprotocollen blijkt dat niet of nauwelijks sprake is van een nadere uitwerking of categorisering van de (bijzondere) persoonsgegevens-verwerking en/of deling bij de verschillende vormen van ondersteuning of hulp die geboden wordt. Ook wordt niet gedefinieerd wat verstaan wordt onder de algemeen geaccepteerde autorisaties- en beveiligingsstandaarden en –normen die voor de betrokken partijen gelden. Het kan voor de instellingen daardoor niet duidelijk welke passende beveiligingsmaatregelen die instellingen zelf moeten nemen. Wel worden de gebruikers van het registratiesysteem geïnformeerd over de door de gemeente geïmplementeerde informatiebeveiligingsmaatregelen (e.g. wachtwoordbeleid, VPN verbinding en gebruikersbeheer voor RIS) waaraan de gebruikers moeten houden.

3.3.4 Werkinstructies

Voor de hulpverleners van Samen DOEN, OKT en Wijkzorg zijn werkinstructies beschikbaar waarin het werkproces voor de hulpverlener beschreven staat. De werkinstructies beschrijven in vaste stappen het proces van de ondersteuning van het huishouden. Deze bevatten geen of beperkte instructies met betrekking tot privacy. In de werkinstructies van Samen DOEN zijn een aantal instructies uitgewerkt, zoals een verzoek op inzage, verbetering, aanvulling, verwijderen of afscherming van gegevens van de cliënt. Het college van B en W heeft aangegeven in de beantwoording van de raadsvragen van september 2015 dat een deugdelijke procedure voor inzage, klachten en bezwaren ingericht wordt.

Voor OKT is een Q&A op de werkwijze beschikbaar gesteld die ingaat op de vraag hoe moet worden omgegaan met het uitwisselen van informatie en privacy.
Naast de werkinstructies zijn er RIS-handleidingen beschikbaar voor het Registratie Informatie Systeem (RIS) die als doel hebben de gebruiker wegwijs te maken in de belangrijkste functies en het verwerken van gegevens in RIS. In de RIS-handleiding

van OKT wordt op diverse plekken aandacht besteed aan het zorgvuldig omgaan met de privacy van cliënten. Tevens wordt in de handleiding verwezen naar het privacyprotocol.

3.3.5 Conclusie

Wanneer we de afspraken met de samenwerkende organisaties toetsen aan de normen van de Wbp (zie paragraaf 3.1) komen we tot de conclusie dat op hoofdlijnen aandacht besteed is aan privacyborging, waardoor in opzet aan de normen wordt voldaan.

In de samenwerkings- en inkoopovereenkomsten zijn weinig tot geen afspraken opgenomen over de wijze waarop met persoonsgegevens dient te worden omgegaan. Nadere afspraken over privacy zijn gemaakt in de privacyprotocollen. Ook de overeenkomsten met de groepspraktijken en vrijgevestigde partijen bevatten bepalingen over privacy, welke niet nader zijn uitgewerkt.

Informatie over de doeleinden, de mate, wijze en bewaartermijn van de gegevensverwerking (norm 1 en 2) van Samen DOEN, OKT en Wijkzorg is in grote lijnen terug te vinden in de privacyprotocollen. De bewaartermijn (15 jaar) voldoet aan de bepalingen uit de Wbp. Ook de rechten van de betrokkenen van de gegevensverwerking zijn beschreven in de privacyprotocollen en duidelijk is gemaakt naar wie zij zich kunnen wenden voor het uitoefenen van deze rechten (norm 3). De gemeente geeft aan dat de protocollen jaarlijks worden beschouwd op eventuele noodzakelijke aanpassingen.

In de privacyprotocollen en werkinstructies ontbreekt het aan een uitwerking en concretisering van de gegevensverwerking bij de verschillende vormen van ondersteuning en hulp die aangeboden wordt binnen Samen DOEN, OKT en Wijkzorg. Een toetsing of een proportionele gegevensverwerking plaatsvindt wordt hierdoor problematisch (norm 1). Ook is niet geconcretiseerd wat verstaan wordt onder de passende beveiligingsmaatregelen die partijen moeten nemen voor gegevensverwerking (norm 4).

Geheimhouding wordt geborgd door de functionarissen die betrokken zijn bij de gegevensverwerking een geheimhoudingsverklaring te laten tekenen (norm 4). Bovendien wordt in de privacyprocollen vermeld dat gebruik gemaakt wordt van autorisaties in het registratie systeem (norm 4).

In de samenwerkingsovereenkomst van Samen DOEN en OKT is opgenomen dat de hulpverlenende instellingen zullen werken met het (voorlopige) registratie informatiesysteem (RIS), maar het verwerken in een ander systeem is niet contractueel uitgesloten. In de overeenkomsten is niet vastgelegd dat de instellingen niet mogen registreren in andere systemen dan het daarvoor bedoelde systeem (RIS en Kidos) voor de uitvoering van Samen DOEN en OKT. Het gevolg hiervan is dat het hiermee de instellingen toelaat (bijzondere) persoonsgegevens ook te verwerken in

andere registratiesystemen waar de gemeente geen zicht op heeft en het risico op privacyschending toeneemt (norm 1).

3.4 Afspraken met leverancier geautomatiseerde systemen

Registratie Informatie Systeem (RIS)
De gemeente maakt voor Samen DOEN, OKT en Wijkzorg gebruik van een digitaal registratiesysteem waarin de (bijzondere) persoonsgegevens van betrokkenen worden geregistreerd, beheerd en verwerkt (in de vorm van dossiers over cliënten of huishoudens). Samen DOEN, OKT en Wijkzorg kennen elk hun eigen afgescheiden RIS-modules die via een webapplicatie benaderd kunnen worden. Voor het management biedt RIS inzicht in de voortgang op het primaire werkproces.

De gemaakte afspraken met de leverancier geven inzicht in hoeverre hiermee de privacy en een adequate gegevensverwerking is gewaarborgd. Het college van B en W is hiervoor verantwoordelijk. Zij stuurt de externe softwareleverancier aan, en houdt toezicht dat de leverancier voldoet aan de organisatorische en technische wettelijke geldende vereisten met betrekking tot de informatiebeveiliging. [150] Deze beveiliging dient passend te zijn bij het niveau waarop (bijzondere) persoonsgegevens worden verwerkt.[151] Hierbij moet men denken aan maatregelen die de persoonsgegevens beveiligen tegen verlies, onrechtmatige verwerking, ongeautoriseerde kennisneming en onnodige verzameling en verdere verwerking van gegevens.

3.4.1 Hoofd- en bewerkersovereenkomst

De gemeente heeft met de leverancier van de RIS-modules van Samen DOEN, OKT en Wijkzorg naast de hoofdovereenkomst, waarin afspraken staan over o.a. de te leveren diensten, verwerking van gegevens conform de Wbp en beveiliging, een bewerkersovereenkomst afgesloten.[152] De leverancier van RIS is *bewerker* in de zin van de Wbp en daarmee degene die ten behoeve van de gemeente persoonsgegevens verwerkt. De bewerkersovereenkomst geeft een aanvulling en aanscherping op de hoofdovereenkomst over de wijze van verwerking van persoonsgegevens, waaronder *de beveiligingsmaatregelen* en *autorisaties* in RIS. In het geval de afspraken in de overeenkomsten door bewerker niet nagekomen worden of in strijd zijn met de Wbp, dan is de bewerker aansprakelijk voor de schade of het nadeel dat daardoor ontstaat.

De leverancier moet de nodige veiligheidsmaatregelen nemen om persoonsgegevens te beschermen. Deze maatregelen moeten in ieder geval voldoen aan de geldende beveiligingsstandaarden voor dit soort gegevensverwerking in de sector.[153] Voor de

[150] Privacyprotocol Samen DOEN, versie 2, 2 oktober 2015; Privacyprotocol OKT, versie 1, 21 september 2015 en privacyprotocol Wijkzorg, versie 2, 25 september 2015
[151] Privacyprotocol Samen DOEN, versie 2, 2 oktober 2015; Privacyprotocol OKT, versie 1, 21 september 2015 en privacyprotocol Wijkzorg, versie 2, 25 september 2015
[152] In de overeenkomst met de leverancier is ook de RIS-module Jeugd en Gezin opgenomen. Deze valt buiten de scope van het onderzoek.
[153] Informatie over de beveiligingsmaatregelen is afkomstig uit Bijlage 2 bij de bewerkersovereenkomst tussen de Gemeente Amsterdam en [leverancier], 16 april 2015 versie 1.3, tenzij anders vermeld.

bewaartermijn van de vastlegging van persoonsgegevens moeten nog nadere procedure- en beheerafspraken gemaakt worden. De afspraken over het proces van autorisatie houden in dat alle RIS-gebruikers van Samen DOEN, OKT en Wijkzorg – voordat zij toegang krijgen tot RIS - een autorisatie- en een geheimhoudings-verklaring moeten tekenen. Voor gebruikers die buiten de gemeentelijke organisatie vallen dient een verklaring omtrent gedrag (VOG) opgevraagd te worden.[154] Inloggen in de RIS-modules gebeurt middels een gebruikersnaam, wachtwoord en SMS tancode[155], en is op verschillende manieren beveiligd.[156]
De leverancier moet rekening houden met het feit dat ook bijzondere gegevens worden verwerkt, alsmede gegevens betreffende de gezondheid waarop een geheimhoudingsverplichting van gebruikers kan rusten. De veiligheidsmaatregelen zijn dan ook ten minste conform de standaard voor informatiebeveiliging, ISO 27001/27002. Om het niveau van beveiliging te bepalen worden de richtsnoeren van het CBP door de bewerker nageleefd.

De leverancier moet zorg dragen voor beveiligingsmaatregelen, zoals een VPN-verbindingen, SSL-certificaten, audit trails op alle transacties, bewaartermijnen en autorisatiebeheer.[157] Daarnaast is de leverancier verantwoordelijk voor de hosting van RIS-modules. Hierbij moet de gemeente rekening houden met het feit dat de bedrijfs-voering van de gemeente, c.q. de feitelijke gebruikers, in gevaar kan komen wanneer de leverancier onverhoopt in de problemen raakt.[158] De partijen hebben naar elkaar toe de intentie uitgesproken te zoeken naar een oplossing waarmee de continuïteit ten aanzien van operationeel blijven van RIS en het kunnen door ontwikkelen van RIS niet in gevaar komt zodra de leverancier onverhoopt in de problemen mocht raken en/of de gemeente de dienstverlening geheel of gedeeltelijk wenst onder te brengen bij een andere partij.[159]

---

[154] Interview, 26 mei 2015.

[155] Dit geldt ook als iemand binnen het gemeentelijk netwerk werkt. De gebruikers van RIS OKT mogen alleen vanaf de OKT Portal inloggen. Dit is een beveiligde Citrix omgeving van OKT waarop de medewerkers moeten inloggen. Ook daar logt men in met een gebruikersnaam, wachtwoord en SMS tancode (bron: feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016).

[156] Na drie verkeerde pogingen om in te loggen wordt het account voor 10 minuten geblokkeerd. Bij meer dan 15 onjuiste inlogpogingen binnen 1 uur zal een gebruiker voor 1 uur geblokkeerd worden (bron: feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016). Bij nogmaals onjuist inloggen wordt het account volledig geblokkeerd. Gebruikers die op een zogenaamde 'whitelist' staan kunnen direct van de RIS-module gebruik maken. De whitelist wordt beheerd door de leverancier. De gemeente kan deze niet zelf aanvullen (bron: interview, 26 mei 2015). Sinds oktober 2015 is het wachtwoordbeleid aangescherpt. Medewerkers dienen nu elke 60 dagen hun wachtwoord te wijzigen (bron: interview, 8 december 2015). Na 180 dagen geen gebruik gemaakt te hebben van RIS, dan vervallen automatisch de rollen, waardoor een gebruiker geen rechten meer heeft in RIS. In RIS Samen DOEN en Wijkzorg wordt een sessie van een gebruiker beëindigd als zij 30 minuten inactief is in de applicatie. In RIS OKT is deze tijdslimiet 15 minuten (bron: feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016).

[157] Bijlage 1 bij de bewerkersovereenkomst tussen de Gemeente Amsterdam en softwareleverancier, 16 april 2015 versie 1.3

[158] Hoofdovereenkomst tussen Gemeente Amsterdam en softwareleverancier., 16 april 2015.

[159] Hoofdovereenkomst tussen Gemeente Amsterdam en softwareleverancier., 16 april 2015.

Penetratie- en hacktest
Binnen de gemeente is de afspraak gemaakt dat standaard bij systemen die via internet toegankelijk zijn en extern worden gehost een pen- en hacktest wordt uitgevoerd door de verantwoordelijke organisatieonderdelen.[160] In de bewerkers-overeenkomst met de leverancier is vastgelegd dat de bewerker (leverancier) jaarlijks middels een penetratie- en hacktest moet aantonen dat de applicatie voldoet aan de richtlijnen voor webapplicatiebeveiliging (de zogenaamde 'OWASP' criteria).
Met een penetratie- en hacktest (binnendringingtest) kunnen computer- en/of registratiesystemen getoetst worden op kwetsbaarheden om in deze systemen in te breken (hacken). De test vindt met toestemming van de gemeente plaats en heeft als doel de systemen beter te beveiligen. De resultaten van de test moeten voorgelegd worden aan de gemeente. Tevens moet de bewerker volledig zijn medewerking verlenen aan een eventuele extra pen- en hacktest zodra de gemeente dit wenst.

Technisch en functioneel beheer
In de hoofdovereenkomst wordt onderscheid gemaakt tussen technisch beheer en functioneel beheer voor de RIS-modules. De leverancier is verantwoordelijk voor het technische beheer van de RIS-modules; het beheer van de applicaties en de databases. De gemeente is verantwoordelijk voor het functioneel beheer.[161] Onder functioneel beheer vallen activiteiten als het verkrijgen van accounts[162], het beheren van de gebruikers, instructies, resetten wachtwoorden, autorisaties intrekken van medewerkers die uit dienst gaan, het op orde houden van de werkprocessen in RIS[163], en andere helpdeskactiviteiten. Ook de verantwoordelijkheid van het verzamelen van wensen van nieuwe aanpassingen (en vertalen naar functioneel ontwerp) ligt bij de gemeente.[164] Het functioneel beheer van de RIS-modules is medio 2015 centraal integraal belegd bij één organisatieonderdeel.[165] Tot dan toe was er per RIS-module apart een functioneel beheerder.[166]

De leverancier zorgt dat de ingevoerde persoonsgegevens in de verschillende RIS-modules automatisch worden opgeslagen in de database van het systeem. Het beheer van de gegevens ligt hij het team Functioneel beheer RIS.[167]

---

[160] Interview, 12 december 2015.
[161] Interview, 26 mei 2015 en mailing, 1 december 2015.
[162] De afdelingshoofden of programmanagers zijn verantwoordelijk voor de autorisaties van onder verantwoordelijke RIS-module (bron: interview, 8 december 2015).
[163] Als een gebruiker bijvoorbeeld een verslag aan een verkeerd dossier gehangen heeft of een verkeerd proces gestart heeft, kan een functioneel beheerder dit herstellen (bron: feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016).
[164] Elke wijziging in RIS OKT wordt voorgelegd aan juristen en PIB-ers (bron: stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016).
[165] Medio 2015 bestaat deze uit een functioneel beheercoördinator die een (klein) team functioneel beheerders aanstuurt voor het beheer van de RIS-modules (bron: feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016).
[166] Interview, 26 mei 2015 en mailing, 1 december 2015.
[167] Bijlage 1 bij de bewerkersovereenkomst tussen de Gemeente Amsterdam en leverancier, 16 april 2015 versie 1.3

In de hoofdovereenkomst is opgenomen dat gegevens ten behoeve van een rapportage verstrekt (kunnen) worden. De gemeente heeft per RIS-module bepaald welke managementrapportages zij wil hebben. De managementrapportages in RIS bevatten alleen geanonimiseerde gegevens.

Autorisaties RIS
Onder verantwoordelijkheid van de gemeente valt ook de koppeling tussen de rechten van RIS-gebruikers en de functionaliteiten in RIS. Deze koppeling houdt in dat gebruikers enkel toegang zouden moeten krijgen tot de informatie waartoe zij op basis van de functies gemachtigd zijn. Voor autorisaties wordt onderscheid gemaakt tussen actieve en passieve gebruikers. Actieve gebruikersaccounts kunnen inloggen in RIS aan de hand van toegekende rechten uit de autorisatiematrix. Passieve gebruikersaccounts zijn gedeactiveerd en kunnen niet meer inloggen in RIS. Deze blijven wel in de RIS database beschikbaar, zodat met terugwerkende kracht managementrapportages kunnen worden opgevraagd. Tevens kunnen deze gebruikersaccounts door de functioneel beheerders opnieuw worden geactiveerd.[168]

De autorisatieniveaus van gebruikers van de RIS-modules zijn opgenomen in de autorisatiematrixen. Bij elke functie, die een medewerkers kan hebben, horen rechten om dossier wel of niet aan te maken, in te zien of te muteren. Deze rechten zijn binnen de autorisatiematrix van RIS gespecificeerd in verschillende rollen. De functioneel beheerder van de gemeente kent rechten toe aan een specifieke gebruiker als een aanmeldformulier is ingediend.[169]

Autorisaties RIS Samen DOEN
Tussen de RIS-modules zitten verschillen in het niveau van toegang van de gebruikers.[170] Zo wordt bij Samen DOEN onderscheid gemaakt tussen de rollen medewerker, teamleider en teamassistent, functioneel beheer, programmateam en servicedesk. De klanthouder bij Samen DOEN (1ste generalist) kan andere gebruikers (bijvoorbeeld de 2e generalist) toegang verlenen tot een cliëntdossier. Het kan ook zijn dat eventueel andere professionals die op basis van het plan van aanpak (bijvoorbeeld een jeugdpsycholoog) betrokken zijn het dossier van een huishouden kunnen inzien of een instelling buiten Samen DOEN een machtiging krijgt om een dossier in te zien (dit komt weinig voor).[171] De teamleiders en teamassistenten hebben volledig toegang tot dossiers behorend tot zijn/haar buurtteam.[172] Teamleiders[173] doen de wijkverdeling en zijn bevoegd om een dossier van een klanthouder toe te wijzen of van klanthouder te veranderen binnen hetzelfde team (bijvoorbeeld bij ziekte of verlof).

[168] Stedelijk directeur sociaal, feitelijk wederhoor, , 15 februari 2016.
[169] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[170] Interview, 26 mei 2015.
[171] Interview, 10 november 2015.
[172] Uniforme Werkwijze Samen DOEN in de buurt versie januari 2015.
[173] Per 17 februari 2016 zijn er 17 teamleiders met te ruime bevoegdheden in RIS Samen DOEN (bron: mail, 17 februari 2016).

Volgens de gemeente moeten de teamleiders de dossiers inzien om te bepalen welke klanthouder het beste aan welke cliënt toegewezen kan worden.[174] De teamassistent[175] dient de administratie te controleren en -in sommige gevallen- het voorwerk te doen voor de generalisten (e.g. de adresgegevens invoeren).176 De teamleiders, teamassistenten en programmamanagers hebben ook een specifieke rol als het gaat om kwaliteitsbewaking[177] en regie bij calamiteiten en incidenten[178], waardoor binnen Samen DOEN gekozen is voor ruimere bevoegdheden.

In de notitie ' "Wat doet u met mijn gegevens?" Zorg voor privacy' wordt aangegeven dat de gemeente geen toegang heeft tot de zorginhoudelijke informatie. Dit blijkt niet overeen te komen met de situatie bij Samen DOEN. Hier hebben de teamleiders en teamassistenten die in dienst zijn van de gemeente wel degelijk toegang tot de deze informatie. Er wordt tevens geen onderscheid gemaakt tussen 'wat' en 'dat' informatie (zie paragraaf 1.2.2) in de dossiers, terwijl het wel om bijzondere persoons-gegevens gaat (w.o. het zelfredzaamheidsmatrix, medische en juridische gegevens van de betrokkenen).

Autorisaties RIS OKT
Bij OKT hebben alleen de hulpverleners toegang tot de inhoudelijke dossiers van cliënten.[179] De klanthouder van een dossier kan meerdere hulpverleners toegang verlenen tot het dossier.[180] De teamleiders van OKT hebben geen toegang tot de gegevens die de hulpverleners verwerken.[181] Zij krijgen in de toekomst wel een autorisatie om in noodgevallen de gegevens in te zien.[182]

Autorisaties RIS Wijkzorg
Binnen RIS Wijkzorg heeft alleen de regisseur toegang tot de gegevens. De regisseur kan meerdere gebruikers toegang verlenen tot het dossier.[183] Elke moederorganisatie binnen Wijkzorg heeft één of meerdere superusers in dienst. De superuser is het eerste aanspreekpunt voor RIS en kan accounts aanvragen. Bij een aanvraag wordt de

---

[174] stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[175] Per 17 februari 2016 zijn er 35 teamassistenten met te ruime bevoegdheden in RIS Samen DOEN (bron: mail, 17 februari 2016).
[176] Interview, 10 november 2015.
[177] Het gaat hier om het bewaken van de kwaliteit en volledigheid van de registraties, maar ook voor het borgen van de (kind)veiligheid. De decentralisatie in het sociaal domein en de een nieuwe werkwijze zorgen ervoor dat kwaliteit (kwalitatief) en coaching en sturing (kwantitatief) vanuit de teamleider een cruciale rol krijgen. Zonder deze vormen van "softcontrol" (c.q. lerende praktijk) is het volgens de gemeente vrijwel onmogelijk te sturen op doelgerichtheid, doelmatigheid en in de laatste plaats rechtmatigheid (bron: Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016).
[178] In deze situaties moeten zij ervoor zorgen dat de informatie toegankelijk is wanneer de betrokken generalist niet bereikbaar of niet in staat is om direct inzage te kunnen geven in gegevens (bron: Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016).
[179] Beantwoording raadsvragen Poorter en Mbarki, 29 september 2015
[180] Softwareleverancier, feitelijk wederhoor, 15 februari 2016.
[181] Interview, 10 november 2015
[182] Interview, 10 november 2015
[183] Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy; Cluster sociaal IV systeem RIS 3D's, versie 1.2, 28 augustus 2014

gebruikersverklaring getekend door de superuser en de gebruiker. De functioneel beheerder maakt vervolgens het account aan.
De backoffice van Wijkzorg is een selecte groep gebruikers die mutaties kunnen doorvoeren in het RIS-systeem.[184] Het betreft hier slechts een specifiek scherm. De gebruikers hebben geen toegang tot het hele dossier.[185]

De medewerkers van de softwareleverancier hebben een eigen RIS-gebruikers-account.[186] De gebruikersrechten van deze medewerkers zijn het lezen, bewerken of verwijderen van dossiers. [187] Deze rechten zijn volgens de gemeente noodzakelijk om fouten in het systeem te kunnen verhelpen. Afgesproken is dat de leverancier een log bijhoudt wie, wanneer en welke dossiers raadpleegt. De leverancier mag alleen dossiers inkijken wanneer de gemeente daartoe opdracht geeft.[188] Als er op database-niveau aanpassingen of conversies moeten worden gedaan, bij een of een groep cliënten, geven de functioneel beheerders daartoe opdracht aan de leverancier.[189] Hoe omgegaan moet worden met deze privacygevoelige gegevens is opgenomen in de bewerkersovereenkomst tussen de gemeente en softwareleverancier. De medewerkers van de leverancier hebben een geheimhoudingsplicht. De CPA heeft aangegeven dat de softwareleverancier nooit gegevens uit de productieomgeving zou mogen kunnen inzien, muteren of verwijderen.[190] Volgens de gemeente zijn de risico's op bovenmatig/onrechtmatig delen van gegevens door de medewerkers van de leverancier in voldoende mate beheerst door de afgesloten bewerkersovereenkomst en de geheimhoudingsplicht van deze medewerkers.[191]

In de beantwoording van de raadsvragen van 29 september 2015 geeft het college van B en W aan dat vastgelegd wordt wie wanneer welk dossier raadpleegt of muteert. Een logsysteem maakt onder andere mogelijk dat de gemeente terug kan zien wie ingelogd heeft en/of wie onrechtmatig inlogt in de RIS-modules. De gemeente is voornemens, zodra er één functioneel beheerder is aangesteld voor alle RIS-modules, dit aspect op te pakken.[192]

3.4.2 Conclusie

Positief is dat zowel voor Samen DOEN, OKT als Wijkzorg gescheiden registratie-systemen geïntroduceerd zijn in plaats van meerdere losse systemen. De gemeente is verantwoordelijk voor het functionele beheer van de registratiesystemen (RIS-modules), en dient de leverancier aan te sturen en moet toezicht houden op de

[184] Interview, 18 maart 2015
[185] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[186] Per 17 februari 2016 gaat het om 12 servicedesk medewerker van de leverancier van RIS (bron: mail, 17 februari 2016).
[187] Mail, 1 december 2015
[188] Interview, 8 december 2015
[189] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[190] Interview, 8 december 2015
[191] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[192] Interview, 18 maart 2015.

leverancier of zij voldoet aan de organisatorische en technische wettelijke geldende vereisten op het gebied van informatiebeveiliging. Hiertoe is een hoofd- en bewerkersovereenkomst met de leverancier van de RIS-modules afgesloten. In de overeenkomsten ontbreekt een concrete beschrijving van de doeleinden van de gegevensverwerking (norm 2; zie paragraaf 3.1) en is de bewaartermijn niet contractueel vastgelegd (norm 1).
Met de leverancier zijn afspraken gemaakt over het door de betrokkenen kunnen beschikken van hun gegevens (norm 3). De RIS-modules worden door verschillende technische maatregelen beveiligd, waaronder een strikt wachtwoordbeleid. Voor de geheimhouding moeten de medewerkers van de leverancier een geheimhoudingsverklaring tekenen (norm 4).

Volgens de CPA mogen softwareleveranciers nooit gegevens uit de productieomgeving inzien, muteren of verwijderen. De medewerkers van de leverancier hebben echter een eigen RIS-gebruikersaccount waarmee ze toegang hebben tot de dossiers van cliënten en deze kunnen muteren. De risico's op bovenmatig/onrechtmatig delen van gegevens zijn hierdoor reëel aanwezig. Dit zorgt bovendien dat extra toezicht op de naleving van privacyafspraken noodzakelijk wordt.

De medewerkers van Samen DOEN hebben te ruime bevoegdheden in RIS. De gemeentelijke functionarissen, zoals teamleiders en teamassistenten, kunnen in zorginhoudelijke informatie van cliënten die voor hun taakuitoefening niet noodzakelijk is. Hier wordt geen onderscheid gemaakt tussen 'dat' en 'wat' informatie, waardoor bijvoorbeeld medische en justitiële gegevens ('dat' informatie) niet alleen voor de daartoe bevoegde medewerkers toegankelijk zijn maar ook voor niet bevoegde medewerkers.

Er moet worden voldaan aan de standaard beveiliging (norm 4). Hier wordt verwezen naar de standaard norm uit de sector, een certificering en de richtsnoeren van het CBP.

3.5 Afspraken voor een lerende organisatie

Hoe heeft het college van B en W richting gegeven aan een 'lerende praktijk'? En worden ervaringen met gegevensverwerking en privacybescherming gebruikt om niet alleen het privacybewustzijn te ontwikkelen en te stimuleren maar ook om op basis daarvan te komen tot een goede balans tussen gegevensverwerking en privacy bescherming? Bij het beantwoorden van deze vragen gaan wij in op de vraag wie verantwoordelijk is voor de lerende praktijk en maken wij onderscheid tussen de concernbrede maatregelen en de specifieke maatregelen op clusterniveau in het sociaal domein.

3.5.1 Verantwoordelijkheden

De CIO-Office is verantwoordelijk voor het opzetten en onderhouden van een concernopleiding voor lokale functionarissen en een intern netwerk voor kennis-

uitwisseling als het gaat om het gebruik van persoonsgegevens en bescherming van de persoonlijke levenssfeer van burgers.[193] Eerder is geconstateerd dat ook de privacycoördinatoren van de clusters een rol hebben in het stimuleren van privacybewustzijn binnen zijn of haar eigen cluster (zie paragraaf 3.2.1).

In de samenwerkingsovereenkomsten van Samen DOEN en OKT is vastgelegd dat de uitvoerende instellingen verantwoordelijk zijn voor de kwaliteit van de te leveren zorg en het opleiden van de teamleden (professionals), teneinde bij te dragen aan het uitvoeren van de maatschappelijke doelen van de gemeente Amsterdam.[194] Voor Samen DOEN brengt de gemeente echter wel een nuancering aan als het gaat om de benodigde kennis voor het uitvoeren van werkzaamheden binnen Samen DOEN; de opleiding en trainingen vallen onder de verantwoordelijkheid van de gemeente. De instellingen zijn verantwoordelijk voor het op peil houden van (vakinhoudelijke) kennis voor hun medewerkers (bijvoorbeeld kennis over verstandelijk gehandicapten).[195] Bij Wijkzorg zijn in de inkoopdocumenten, die als bijlage worden opgenomen in de raamovereenkomst met de zorgaanbieders, specifieke eisen gesteld aan het personeel (diploma's, certificering, etc.).[196] De verantwoordelijke voor opleiding/scholing wordt niet benoemd.

3.5.2 Concernbreed

CISO heeft, onder verantwoordelijkheid van de CIO-Office, op het gebied van informatiebeveiliging en privacy een cursus risicoanalyse ontwikkeld. De methodiek van de cursus is overgenomen door de VNG. In de cursus worden medewerkers getraind in het uitvoeren van de risicoanalyses die onderdeel zijn van het PPM-proces.[197]

3.5.3 Cluster Sociaal

Voor Samen DOEN, OKT en Wijkzorg wordt in verschillende beleidsdocumenten uiteengezet hoe zich een lerende praktijk moet ontwikkelen. De inrichting wijkt op enkele punten van elkaar af bij de verschillende organisaties. Verschillen zitten onder meer in de wijze waarop Samen DOEN, OKT en Wijkzorg hun leerlijn hebben vormgegeven, de eventuele actoren die een rol vervullen bij de lerende organisatie, de casuïstiekoverleggen en de privacyschouw Jeugd. Alleen OKT valt binnen de scope van de privacyschouw Jeugd.[198]

---

[193] Notitie 'Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens', 8 november 2011

[194] Samenwerkingsovereenkomst Samen DOEN in de buurt, oktober 2014, art. 11; Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014, art. 12

[195] Interview, 26 oktober 2015

[196] Inkoopdocument Wmo 2016, AIS-2015-0009 (bijlage van Raamovereenkomst Wmo 2015)

[197] Interview, 12 december 2015.

[198] Feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016.

Leerlijn
Leren en ontwikkelen wordt bij Samen DOEN opgevat als een 'lerende organisatie'; leren is een continu proces. Het kan zowel het gevolg zijn van ontwikkelingen in de organisatie of het kan nieuwe ontwikkelingen teweeg brengen. Voor de organisatie betekent dit dat behalve in het opleiden van medewerkers wordt geïnvesteerd, de medewerkers ook worden betrokken bij het verbeteren van de werkwijze op basis van ervaringen uit de praktijk. Het leerproces binnen Samen DOEN wordt op meerdere niveaus gestalte gegeven; via de dagelijkse professionele praktijk, het gedrag en de werkwijze van de hulpverleners en relaties tussen hulpverleners en tot slot tussen de teams en het programmateam Samen DOEN.[199]

Om er zorg voor te dragen dat nieuwe inzichten, ervaringen en 'best practices' een structurele plek in het programma krijgen en geleerd wordt van dilemma's en belemmeringen is de volgende leerroute uitgezet: [200]
- Dilemma's, successen en belemmeringen worden zowel binnen de teams als met het programmateam van Samen DOEN gedeeld;
- Uit deze inzichten worden lessen getrokken door zowel het programmateam als de uitvoerende teams;
- De resultaten hiervan worden, waar relevant, zowel op teamniveau als op programmateam-niveau geïmplementeerd.

Samen DOEN professionals leren in de praktijk op twee manieren over het onderwerp privacy; in de leerlijn en door middel van casuïstiekbespreking. Met de verdiepingsmodules uit de leerlijn kunnen Samen DOEN teams specifieke expertise ontwikkelen en onderhouden.[201] De leidinggevende regelt dat de nieuwe medewerker op de hoogte is van de wijze waarop processen worden uitgevoerd en de wijze waarop RIS dient te worden gebruikt.[202] In deze RIS-training wordt aandacht besteed aan de hoofdlijnen van het privacybeleid en worden casusspecifieke privacyvragen beantwoord.[203]

Zowel in het koersbesluit[204] Om het kind, waarin de Ouder- en Kindteams zijn vorm-gegeven, als in het programmaplan[205] is uitgesproken een basis te leggen voor een lerend systeem. Met deze leerlijn moeten krachtige teams ontstaan door middel van reflectie vanuit de uitvoeringspraktijk op het systeem van de zorg voor de jeugd, en moeten professionals zich blijvend ontwikkelen en scholen. In de leerlijn van de OKT en moeten professionals zich blijvend ontwikkelen en scholen. OKT organiseert privacyworkshops voor de hulpverleners in twee varianten: één met een open inschrijving voor alle medewerkers van OKT en daarnaast incidentele work-

[199] Visie op leren en ontwikkelen: De Samen DOEN in de buurt leerlijn, juli 2013.
[200] Visie op leren en ontwikkelen: De Samen DOEN in de buurt leerlijn, juli 2013.
[201] Gebundelde krachten: Evaluatie Samen DOEN in de buurt in Amsterdam, oktober 2014, blz. 10.
[202] Uniforme Werkwijze Samen DOEN in de buurt versie januari 2015, blz. 45.
[203] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[204] Koersbesluit Om het Kind, 15 mei 2013.
[205] Programmaplan II (2013 – 2014) Om het Kind,19 maart 2013 .

shops voor individuele teams. Daarnaast heeft OKT ook een RIS-training waar privacy aan bod komt.[206]

Voor professionals van Wijkzorg wordt een basis gelegd voor een leerlijn door meer samenhang te gaan bieden tussen de losse trainingen en instructies voor het omgaan met RIS en instrumenten zoals de zelfredzaamheidsmatrix (ZRM) en het ondersteuningsplan. [207] Voor de optimalisering van huidige trainingen en de ontwikkeling van nieuwe trainingen wordt geïnventariseerd welke behoeften er zijn vanuit het veld. De ontwikkeling van deze basisleerlijn wordt door de gemeente in samenwerking met de veldpartijen aangegaan.[208] Om professionals in staat te stellen de nieuwe werkwijze van Wijkzorg goed uit te voeren, worden verschillende activiteiten door de gemeente ingezet. Voor een deel waren deze activiteiten al gepland, andere zijn extra ingezet naar aanleiding van signalen uit de wijkteams. Dit laatste geldt bijvoorbeeld voor het inrichten van het inmiddels opgeheven stedelijk kennisteam Wijkzorg.[209]

Casuïstiekoverleggen
In de casuïstiekoverleggen van Samen DOEN, OKT en Wijkzorg worden in multidisciplinair teamverband verschillende onderwerpen besproken waar de hulpverleners in de praktijk tegenaan lopen . Door het multidisciplinaire karakter van de teams kunnen in veel gevallen binnen het team oplossingen gevonden worden voor de ingebrachte vraagstukken. [210] Bij Samen DOEN hebben de teamleiders bovendien de mogelijkheid een vraagstuk mee te nemen naar het zogenaamde 'community practice overleg' (cop-overleg).[211] Dit is het casuïstiekoverleg voor teamleiders van Samen DOEN. De teamassistenten van Samen DOEN hebben een vergelijkbaar overleg. Daarnaast komen de teamassistentes en teamleiders van Samen DOEN met regelmaat bijeen om privacyvraagstukken te bespreken. Oplossingen voor privacyvraagstukken worden door de teamleiders en -assistenten teruggekoppeld naar de teamleden.[212]

---

[206] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[207] Stand van zaken en ervaringen met Wijkzorg, commissie flap raadscommissie voor Zorg en Welzijn en Sport en Recreatie, 25 juni 2015.
[208] Stand van zaken en ervaringen met Wijkzorg, commissie flap raadscommissie voor Zorg en Welzijn en Sport en Recreatie, 25 juni 2015.
[209] Stand van zaken en ervaringen met Wijkzorg, commissie flap raadscommissie voor Zorg en Welzijn en Sport en Recreatie, 25 juni 2015. Het multidisciplinaire stedelijke kennisteam Wijkzorg was het aanspreekpunt voor professionals van Wijkzorg met inhoudelijke vragen over -het gemeentelijk gefinancierde deel- van Wijkzorg. Daarnaast zorgde het kennisteam ervoor dat de bestaande kennis over de werkwijze van Wijkzorg wordt uitgebreid en beschikbaar werd gesteld. Het kennisteam heeft gefunctioneerd tussen februari en november 2015 en is opgeheven omdat het aantal vragen dat binnenkwam bij het kennisteam minimaal was (bron: Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016).
[210] Interview, 10 november 2015.
[211] Interview, 10 november 2015.
[212] Interview, 17 november 2015.

Aanspreekpunten en aandachtsfunctionarissen
De privacycoördinator van Samen DOEN[213] is voor de medewerkers/hulpverleners binnen Samen DOEN aanspreekpunt voor privacyvraagstukken. Samen DOEN heeft daarnaast aandachtsfunctionarissen binnen de teams aangesteld, onder meer voor het thema privacy. Zij zijn aanspreekpunt en verantwoordelijk voor het coachen en informeren van hun collega's.[214] De privacycoördinator van Samen DOEN verspreidt relevante informatie naar aanleiding van vragen uit de praktijk binnen de gehele organisatie, per mail of door deze te bespreken in de juridische werkgroep privacy of het programmateam van Samen DOEN. Het kan ook zijn dat deze informatie leidt tot een aanpassing van het beleid, processen en werkinstructies (bijvoorbeeld aanpassingen in het privacyprotocol).[215] Bij OKT en Wijkzorg is dit nog niet op deze wijze georganiseerd. Bij OKT is de adviseur kwaliteit het aanspreekpunt voor privacy. Een vergelijkbare privacycoördinator zoals bij Samen DOEN zijn bij OKT en Wijkzorg niet aangesteld.

Privacyschouw Jeugd
Het college heeft in juni 2015 besloten om de privacyschouw Jeugd uit te voeren.[216] De privacyschouw is voortgekomen uit de notitie ' "Wat doet u met mijn gegevens?"Zorg voor de privacy'.[217] Middels de privacyschouw wordt, vanuit een burgerperspectief, de omgang met gegevens van burgers in het Jeugddomein in beeld gebracht en getoetst.[218] De privacyschouw richt zich op OKT en vooralsnog niet op Samen DOEN en Wijkzorg.[219] Er is overwogen de privacyschouw voor het gehele sociale domein uit te voeren, maar dit zou volgens de gemeente een te grote omvang krijgen.[220] Voor de start van de schouw is overleg geweest met het CBP. Het CBP neemt niet actief deel, maar heeft wel toegezegd informeel te reageren op de uitkomsten zodra deze beschikbaar zijn.[221] De privacyschouw kent vier fasen: een (al uitgevoerde) nulmeting, aanbrengen van de noodzakelijke aanvullingen of verbeteringen (op basis van de resultaten) uit de nulmeting in het proces, het laten uitvoeren van een externe meting door een extern bureau, en tot slot een eindrapportage.[222]

3.5.4 Conclusie
Het college van B en W poogt richting gegeven aan een 'lerende praktijk' door zowel op concern- als clusterniveau niet alleen het privacybewustzijn te ontwikkelen en te stimuleren door opleidingen en cursussen, maar ook door op basis van de ervaringen van hulpverleners uit de praktijk te komen tot een goede balans tussen de mate van

[213] Hier gaat het niet om de privacycoördinatoren van het cluster, maar de privacycoördinator die binnen het programma Samen DOEN actief is.
[214] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[215] Interview, 26 oktober 2015.
[216] Rapport Nulmeting Privacyschouw Jeugd Amsterdam, september 2015.
[217] Staf Flap, Agendapunt, 18 mei 2015.
[218] Eerste tussentijdse rapportage fase Nulmeting "Privacyschouw Jeugd Amsterdam", 17 augustus 2015.
[219] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[220] Interview, 3 december 2015.
[221] Staf Flap, Agendapunt, 18 mei 2015.
[222] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.

gegevensverwerking en privacybescherming. De verantwoordelijkheid wordt daarbij zowel bij CIO-Office, als de privacycoördinatoren van het cluster Sociaal en de uitvoerende partijen belegd, wat de taakverdeling diffuus maakt. In de inkoop-documenten met betrekking tot Wijkzorg is niets vermeld over een verantwoordelijke voor scholing en opleiding. Daarbij wordt ervan uitgegaan dat de hulpverleners hun verantwoordelijkheid nemen en advies of ondersteuning vragen rond vraagstukken uit de praktijk.

De opleidingen en cursussen kunnen indirect bijdragen aan de doelstelling dat de gemeente voldoet aan de Wbp (norm 1 t/m 4) door privacybewustzijn creëren en te versterken onder de medewerkers en te werken volgens wet- en concernafspraken rondom privacy. Op concernniveau is dit met enkel de cursus risicoanalyse zeer summier vormgegeven. Zeker als bedacht wordt dat de focus van de cursus niet nadrukkelijk privacy is.

Binnen het cluster Sociaal is de aandacht voor privacy in de leerlijn vrij diffuus. Alleen bij OKT komt privacy expliciet in de leerlijn terug door middel van de workshop privacy. Voor de leerlijnen van Samen DOEN en Wijkzorg is dit niet of beperkt het geval. Wel komt privacy impliciet terug in de RIS trainingen van Samen DOEN en OKT en in de werkwijze van Samen DOEN. Binnen Samen DOEN is een aparte privacycoördinator aangesteld en zijn er in de wijkteams aandachtsfunctio-narissen met privacy als aandachtsgebied actief. Deze laatste hebben de taak vragen te beantwoorden over privacy en privacybewustzijn te verhogen. De casuïstiekover-leggen hebben belangrijke bijdragen in het onderling van elkaar leren als het gaat om privacyvraagstukken. Dit kan vervolgens haar weg vinden in wijzigingen in beleid of procedures, maar het biedt nog onvoldoende garantie dat dit ook gebeurt. Als extra maatregel heeft het college besloten om de privacyschouw Jeugd uit te voeren.[223] Deze heeft echter geen betrekking tot het gehele cluster Sociaal.

3.6 Conclusie

In deze paragraaf gaan wij in op de vraag of de afspraken ertoe bijdragen dat de privacy in *opzet* is geborgd. De gemeente heeft meerdere organisatorische en technische maatregelen genomen om in opzet zorg te dragen dat aan de Wbp wordt voldaan. De actoren die een belangrijke rol spelen rondom privacy, zoals de privacycoördinatoren, Cluster Advies Teams (CAT) en de Commissie Persoonsgegevens Amsterdam (CPA), voorzien de lijn van (vrijblijvend) advies rondom privacyvraagstukken. Bij het niet opvolgen van het advies van de Commissie Persoonsgegevens Amsterdam (CPA) kan er naar de ambtelijk en/of bestuurlijk verantwoordelijke worden geëscaleerd. De privacycoördinatoren zijn ervoor verantwoordelijk dat de organisatie tenminste voldoet aan de Wbp en de concernafspraken over privacy (norm 1-4; zie paragraaf 3.1). De bevoegdheden zijn

[223] Rapport Nulmeting Privacyschouw Jeugd Amsterdam, september 2015.

echter niet toereikend om deze verantwoordelijkheid waar te kunnen maken; ze zijn niet bevoegd om te beslissen, omdat dit belegd is in de lijn.
Gedurende het Project Portfolio Management (PPM) proces houdt CIO-Office toezicht op de opvolging van de adviezen van de CAT. Daarbij is een onderscheid zichtbaar in de aandacht voor bestaande en nieuwe gegevensverwerking. Het PPM proces is enkel bedoeld voor nieuwe ICT- en informatievoorziening (IV) projecten en niet voor bestaande gegevensverwerking; de monitorende rol ligt in dat geval bij de privacy-coördinatoren van het betreffende cluster, welke functioneel aangestuurd worden door de Chief Information Security Officer (CISO). De instrumenten van de risico-analyses zijn niet bedoeld voor de toetsing op de naleving van wet- en regelgeving in de praktijk ('compliance'). Ook wordt onvoldoende toezicht gehouden op de opvolging van adviezen van de CPA en is het de vraag of zij altijd benaderd worden voor privacyvraagstukken. De CPA heeft hier geen adequaat instrument voor. De jaarlijkse Wbp monitor is volgens de CPA weliswaar bedoeld om privacyrisico's binnen de gemeentelijke organisatie te signaleren en zicht te krijgen op de gegevens-verwerkingen binnen de organisatie, maar is niet het geschikte instrument om de volledigheid en de daadwerkelijke opvolging van adviezen te bewaken.

Bij de afspraken met de samenwerkende organisatie constateren we dat aan drie van de vier normen op hoofdlijnen bij de privacyprotocollen wordt voldaan (norm 2-4). Het ontbreekt regelmatig aan concretisering van vage bepalingen uit de privacy-protocollen en de Wbp. Deze zijn vaak niet uitgewerkt in de werkinstructies van Samen DOEN, OKT en Wijkzorg (norm 1). In de gemaakte afspraken met de samenwerkende organisatie wordt bij Samen DOEN en OKT niet uitgesloten dat ook in andere dan de toegestane registratiesystemen bijzondere persoonsgegevens worden verwerkt (norm 1). Hierdoor neemt het schenden van privacy toe.

We zien het als positief dat de gemeente drie losse registratiesysteem (RIS) gebruikt voor Samen DOEN, OKT en Wijkzorg. Bij de afspraken met de leverancier van het Registratie Informatie Systeem (RIS) ontbreekt het aan nadere afspraken over bijvoorbeeld bewaartermijnen, certificering en continuïteitsplan. We constateren dat de medewerkers van de leverancier van RIS en van de gemeente te ruime bevoegd-heden hebben waardoor ze toegang hebben tot de dossiers van cliënten die voor hun taakuitoefening niet noodzakelijk zijn.

De gemeente heeft zich vanuit verschillende hoeken ingezet om een lerende praktijk te ontwikkelen. Op concernniveau zijn de training en opleidingen beperkt vorm-gegeven. Binnen het cluster Sociaal de aandacht voor privacy in de leerlijn vrij diffuus. OKT heeft inmiddels een workshop privacy die een structureel onderdeel is van de leerlijn. Positief is dat bij Samen DOEN functionarissen zijn aangewezen die privacy als aandachtsgebied hebben en zodoende privacy onder de aandacht moeten brengen bij de hulpverleners. Ook komt privacy terug in de RIS trainingen van Samen DOEN en OKT en in de werkwijze van Samen DOEN.

De belangrijkste vraagbaken voor privacyvraagstukken bij Samen DOEN, OKT en Wijkzorg lijkt in opzet de casuïstiekoverleggen. Hier wordt in onderling verband naar oplossingen gezocht voor privacyvraagstukken. Structureel terugkerende vragen/problemen moeten echter dan wel een weg vinden in de eventuele verbetering van de processen en werkinstructies. Er is geen garantie dat dit daadwerkelijk gebeurt. Bij Samen DOEN zijn hier stappen gezet in de vorm van de juridische werkgroep privacy waar leden van het programmateam en hulpverleners samenkomen.

Het initiatief voor de privacyschouw van het jeugdstelsel zal zeker bijdragen aan het privacybewustzijn binnen de gemeente en haar partners. Met de privacyschouw wordt, vanuit een burgerperspectief, de omgang met gegevens van burgers in het jeugddomein in beeld gebracht en getoetst. De scope van de privacyschouw is echter wel beperkt tot het jeugdstel en niet het hele sociale domein.

4 Hoe worden de organisatorische maatregelen uitgevoerd in de praktijk

In dit hoofdstuk wordt uiteengezet hoe de afspraken die door of namens het college zijn gemaakt over de gegevensverwerking en de omgang met privacy (zie hoofdstuk 3) in de *praktijk* uitpakken. Deze onderzoeksvraag is beantwoord aan de hand van de volgende deelvragen:

1. Hoe worden de afspraken toegepast die binnen de organisatie zijn gemaakt over gegevensverwerking en privacy?
2. Hoe worden de afspraken toegepast die met samenwerkende organisaties zijn gemaakt over gegevensverwerking en privacy?
3. Hoe worden de afspraken toegepast die met de leverancier van de geautomatiseerde systemen zijn gemaakt over gegevensverwerking en privacy?
4. Hoe worden de afspraken toegepast voor een lerende organisatie over gegevensverwerking en privacy?

De structuur van dit hoofdstuk is gelijk aan dat van hoofdstuk 3. De onderzoeksvragen worden in de gegeven volgorde behandeld. Aan het einde van elke paragraaf wordt de werking in praktijk getoetst met de normen uit de Wbp. Deze normen zijn in het kort terug te vinden in paragraaf 3.1. Het volledige normenkader is opgenomen in Bijlage 2 - Normenkader Wet bescherming persoonsgegevens (Wbp).

4.1 Afspraken binnen de organisatie

In deze paragraaf zullen we ingaan op de uitvoering van de binnengemeentelijke afspraken die zijn gemaakt om in opzet te komen tot een adequate gegevensverwerking en een respectvolle omgang met privacy. Eerst worden de privacycoördinatoren behandeld omdat zij een belangrijke sleutelfunctie vervullen bij de uitvoering. Daarna wordt ingegaan op de andere binnengemeentelijke afspraken.

4.1.1 Privacycoördinatoren

Binnen de informatievoorziening eenheid van het cluster Sociaal (IVE Sociaal) zijn drie Privacy- en Informatiebeveiligers (PIB-ers) werkzaam, die een coördinerende rol heeft en aanspreekpunt is voor de andere PIB-ers (bijvoorbeeld voor de managers van het cluster en voor de CISO vanuit de CIO-Office).[224] De privacycoördinatoren hebben het takenpakket zoals omschreven in paragraaf 3.2.1. De functionarissen zijn werkzaam voor alle rve's van het cluster. In de praktijk is dit voornamelijk voor de rve GGD (Gemeentelijke Gezondheidsdienst), WPI (Werk, Participatie en Inkomen) en OJZ (Onderwijs, Jeugd en Zorg).[225]

Specifiek met betrekking tot de samenwerkende partijen laat de praktijk het volgende beeld zien: voor Samen DOEN is reeds een aparte privacycoördinator aangesteld die

[224] Interview, 30 november 2015

[225] Interview, 30 november 2015

aanspreekpunt is voor privacy binnen Samen DOEN. Deze privacycoördinator neemt deel in de juridische werkgroep Samen DOEN (zie paragraaf 2.4.2) en verzorgt de communicatie als het gaat om privacy naar de wijkteams van Samen DOEN (bijvoorbeeld aanpassingen in de processen en het verspreiden van het privacy-protocol).[226] Voor Wijkzorg is geen aparte functionaris beschikbaar waar de ambtelijke organisatie en hulpverleners terecht kunnen voor vragen over privacy.[227] Ook OKT heeft geen vergelijkbare privacycoördinator zoals deze bij Samen DOEN is aangesteld. [228] Het is voor OKT onduidelijk of er een privacycoördinator is vanuit de gemeente die als aanspreekpunt dient voor OKT.[229] Bij Wijkzorg blijkt voornamelijk een onduidelijkheid te bestaan over (de rol van) de privacycoördinatoren van het cluster Sociaal. Voor de decentralisaties kon Wijkzorg direct terecht bij functionarissen voor Privacy en informatiebeveiliging (PIB) voor vragen rondom privacy, nu niet meer.[230]
Het in november 2015 opgezette vakoverleg Privacy (zie paragraaf 2.4.2), waar onder andere de CISO en de cluster PIB-ers samenkomen, draagt er aan bij dat concernbreed afstemming plaatsvindt over privacyvraagstukken. Bovendien kan dit bijdragen aan een betere vindbaarheid van de privacyfunctionarissen binnen de gemeente.

De IVE Sociaal meldt in november 2015 dat zij onvoldoende (personele) capaciteit beschikbaar heeft en dat de werkdruk binnen de IVE Sociaal als hoog wordt ervaren.[231] Hierdoor blijven volgens de IVE Sociaal taken liggen. De PIB'ers hebben meerdere malen aangekaart dat extra capaciteit noodzakelijk is.[232] De extra benodigde capaciteit was bij de IVE Sociaal niet in beeld, omdat de IVE geen zicht had op het totale werkaanbod van de IVE.[233] De IVE Sociaal geeft aan dat de taken in het kader van de verwerking van persoonsgegevens bij voorbaat prioriteit krijgen.[234] In februari 2016 weet de IVE Sociaal ons te melden dat het capaciteitsvraagstuk rondom de PIB'ers inmiddels duidelijk in beeld is. Middels externe inhuur wordt thans een oplossing gezocht.[235]

4.1.2 Project Portfolio Management

Uitgebreide risicoanalyses informatiebeveiliging en privacy (URA)
De informatiebeveiliging en de borging van privacy in de RIS-modules van de drie decentralisaties (w.o. RIS Samen DOEN, OKT en Wijkzorg) is door de gemeente in 2014 getoetst aan de hand van een uitgebreide risicoanalyse (URA). Dit vanwege de grote hoeveelheid (bijzondere) persoonsgegevens die in RIS worden verwerkt. Er is in juli 2014 een concept versie en in september 2014 een definitieve versie voorgelegd

[226] Interview, 26 oktober 2015.
[227] Interview, 11 november 2015.
[228] Interview, 11 november 2015.
[229] Interview, 11 november 2015.
[230] Interview, 11 november 2015.
[231] Interview, 30 november 2015.
[232] Interview, 30 november 2015.
[233] Interview, 30 november 2015.
[234] Interview, 30 november 2015.
[235] Stedelijk directeur sociaal, feitelijk wederhoor, , 15 februari 2016.

aan de Commissie Persoonsgegevens Amsterdam (CPA). De URA laat de volgende resultaten zien:

- zorgverleners zijn zich over het algemeen goed bewust van de gevoelige informatie waarmee ze werken.
- goede trainingen in het gebruik van het systeem en aanvullende bewustwording zijn nodig om eventuele fouten te voorkomen. Als medewerkers niet de juiste opleiding krijgen in het gebruik van RIS en het waarom registreren in RIS tijdens het proces niet duidelijk is, is het mogelijk dat er verkeerd gebruik wordt gemaakt van het systeem.
- als onbevoegden toegang weten te krijgen tot de RIS is de schade hoog. Door regelmatig checks op de beveiligingsmaatregel uit te voeren, kan deze kans verlaagd worden.
- Er zijn vrije invoervelden in RIS waardoor het risico bestaat op bovenmatige vastlegging van gegevens. Door informatie in de vrije velden te plaatsen die niet voor iedereen geschikt is maar niet gefilterd kan worden bij de autorisaties, is het mogelijk dat onbevoegden toegang krijgen tot deze informatie.
- Er zijn veel verschillende ketenpartners die gebruik maken van RIS: duidelijke werkprocedures/gebruikersinstructies zullen voor alle gebruikers van het systeem beschikbaar moeten zijn. De procedures voor het toekennen en intrekken van autorisaties moeten eenduidig zijn.

Deze uitkomsten gaven aanleiding enkele maatregelen te formuleren die in de tweede helft van 2014 in de organisatie zijn geïmplementeerd.[236] De analyse heeft volgens de gemeente geleid tot een beveiliging die boven de norm van de BIG (zie paragraaf 2.4.2) ligt.[237]

Privacy Impact Assessment
Naast de uitgevoerde URA uit 2014 is in dezelfde periode, in opdracht van de gemeente Amsterdam, een PIA door een externe partij uitgevoerd op de gegevensverwerking van Samen DOEN, OKT en Wijkzorg.[238] De focus van de PIA was de gegevensverwerking die plaatsvindt in RIS met de werkwijzen van de betreffende teams op dat moment.

Voor de PIA op de RIS-modules is gekozen om een aparte vragenlijst op te stellen die met enkele aanpassingen in grote lijnen aansluit met de PIA vragenlijst die de gemeente standaard hanteert. De vragenlijst is aan hand van interviews en schriftelijke rondes door geselecteerde belanghebbenden (projectleiders of –medewerkers direct betrokken bij de dagelijkse gang van zaken in de teams en de inrichting en ontwikkeling van de werkwijze van de teams) beantwoord. Daarnaast is input gebruikt van de ICT-ondersteuning/beheerders van de onderscheiden modules en informatie vergaard bij de betrokken juristen.

[236] Interview, 3 december 2015

[237] "Wat doet u met mijn gegevens?" Zorg voor de privacy, versie februari 2015

[238] Privacy Impact Assessment: RIS modules Om het Kind, Samen DOEN en Wijkzorg, 20 augustus 2014

In de uitgevoerde PIA is een beschrijving gegeven van de relevante situaties en elementen van de werkwijze van de teams, de privacyrisico's die daarin worden waargenomen en zijn aanbevelingen voor maatregelen gegeven die gesignaleerde risico's kunnen beperken of ondervangen en algemene aandachtspunten voor de inrichting.[239] De risico's en aanbevelingen voor maatregelen zijn weergegeven aan de hand van verschillende toetsdomeinen (waar onder de werkwijze van de teams, de inrichting van de organisatie, de te verwerken gegevenssoorten, de gekozen ICT voor de gegevensverwerking, beveiliging en de rechten van burgers).

De PIA toonde de het volgende aan:

- Belangrijk aandachtspunt is het vaststellen van de verantwoordelijkheid voor de gegevensverwerking zoals in de Wbp bedoeld voor de registratie in cliëntgegevens.
- Het is van belang dat de gemeente voor bijzondere situaties (zoals in het geval van drang), die relatief meer voor zullen komen bij Samen DOEN, duidelijke criteria vaststelt over wanneer en welke gegevens verwerkt worden en welke waarborgen getroffen worden.
- CPB heeft in richtsnoeren voor beveiliging van persoonsgegevens eisen omtrent beveiliging uitgewerkt. CBP noemt daarvoor het inrichten van een Plan-Do-Check-Act cyclus. Daarmee wordt een reguliere controle, evaluatie en zo nodig bijstelling van beveiligingsmaatregelen geborgd in het primaire proces. Het is van belang dat de gemeente dit proces in de organisatie inbedt.

De belangrijkste conclusies uit de PIA zijn verwerkt in de privacyprotocollen die door het management van OJZ in november 2015 zijn vastgesteld voor Samen DOEN, OKT en Wijkzorg.[240] De PIB'ers hebben een rol om de beheersmaatregelen uit de PIA te monitoren.[241] Echter wordt door IVE Sociaal aangegeven dat niet alles wordt gemonitord. Wat wel of niet gemonitord wordt is op dit niet duidelijk aan te geven.[242]

Opstellen transparantiedocumenten
De transparantiedocumenten van Samen DOEN[243] en Ouder- en Kindteams [244] zijn qua opzet uniform aan elkaar.

Opgenomen in het transparantiedocument is dat de hoofdverantwoordelijke voor de juiste omgang van persoonsgegevens in RIS Samen DOEN de rve OJZ is. Bij OKT is deze verder belegd bij de afdeling Jeugd. Als wettelijke grondslag voor het gebruik van BRP-gegevens bij OKT wordt de Jeugdwet genoemd. De beschrijving van de grondslag voor de gegevensverstrekking bij Samen DOEN wordt niet concreet in het transparantiedocument beschreven (in paragraaf 5.1.1 zal nader ingegaan worden op

[239] Privacy Impact Assessment: RIS modules Om het Kind, Samen DOEN en Wijkzorg, 20 augustus 2014.
[240] Interview, 3 december 2015.
[241] Interview, 30 november 2015.
[242] Interview, 30 november 2015.
[243] Transparantiedocument SD versie 1.1, 28 november 2014
[244] Transparantiedocument OHK versie 1.0, 28 november 2014

de grondslagen voor gegevensverwerking). De werkwijzers worden aangehaald om de vragen te beantwoorden bij welke processen de BRP-gegevens worden gebruikt, wat er mee gebeurt en hoe en door wie de gegevens gebruikt en opgeslagen. Voor RIS Samen DOEN is beschreven dat alleen teamleiders en teamassistenten toegang hebben tot de BRP-gegevens. Bij RIS OKT mogen Ouder- en Kindadviseurs beperkt in de BRP raadpleegschermen. Alle gebruikers dienen zich te houden aan het Addendum Privacy (welke verwijst naar het privacyprotocol) toegevoegd bij de samenwerkingsovereenkomst. Ook hebben ze allen een geheimhoudingsdocument ondertekend.

Voor beide modules is opgenomen dat de bewaartermijnen niet geautomatiseerd zijn in RIS. Gegevens hebben een bewaartermijn van maximaal 15 jaar.
De melding aan het CBP van Samen DOEN vindt plaats in het 4e kwartaal van 2014. Het meldingsnummer wordt in het transparantiedocument verwerkt zodra dat verkregen is. Voor RIS OKT zal de melding bij het CBP in het 1e kwartaal 2015 geschieden. Er is geen geactualiseerde versie van de transparantiedocumenten beschikbaar gesteld door de gemeente. Het transparantiedocument van OKT wordt momenteel geactualiseerd.[245]

4.1.3 Regeling Risicovolle Projecten

In oktober 2014 is voor het laatst aan het college van B en W en de Raad gerapporteerd over de voortgang en risico's van de decentralisaties. In de rapportage wordt gesteld dat privacy en informatiebeveiliging zeer belangrijke uitgangspunten zijn voor de informatievoorziening.[246] Het voorkomen van ongeoorloofde toegang door derden tot bijvoorbeeld een dossier vraagt niet alleen om een (in de technische zin) goed ontworpen informatiesysteem, maar ook om strenge beveiliging in de zin van autorisaties op het dossier. Geconcludeerd wordt dat de applicatie RIS technisch gezien goed ontworpen is en qua beveiliging van vertrouwelijke informatie op het niveau staat van internetbankieren.

Aan de organisatorische kant van de privacy en informatiebeveiliging zijn maatregelen van juridische aard (privacyprotocollen, convenanten etc.) en structurele aandacht voor een cultuuromslag nodig. Benoemd wordt dat er een cultuur moet ontstaan waarin het leidend principe is dat er geen gesprekken over kinderen plaatsvinden, zonder dat ouders hiervoor toestemming hebben verleend.
In de rapportage wordt ingegaan op een aantal keuzes die de gemeente heeft gemaakt, de gevolgen die dat heeft en vragen en risico's worden benoemd. Een van de vragen die gesteld wordt betreft wie de verantwoordelijke is in de zin van de Wbp; daarover is advies aangevraagd (zie ook paragraaf 4.1.2; *Privacy Impact Assessment*).

Ook wordt geconstateerd dat ten gevolge van de keuze voor verschillende RIS-modules enkele generieke taken, zoals leveranciersmanagement, privacy,

[245] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.

[246] Zie: Voortgangsrapportage risicomanagement sociaal domein: Voortgang en risico's van de decentralisaties Jeugdwet, AWBZ/Wmo, Participatiewet, de samenhang tussen de drie decentralisaties (3D), Samen DOEN en Dragende samenleving, oktober 2014

informatiebeveiliging en koppeling met GBA zijn versnipperd, de gebruikers-ondersteuning vanuit één punt ontbreekt en nieuwe ontwikkelingen niet goed worden getest omdat de impact over en weer niet doorzien wordt. Een van de aanbevelingen is een duidelijke governance structuur te ontwikkelen om het functioneel beheer te gaan opzetten.

Expliciet wordt in de rapportage vermeld dat de regels omtrent privacy onvoldoende nageleefd worden. De medewerkers registreren nog (te veel) medische klantgegevens. Hierbij schendt de gemeente de regelgeving/beleid. Aanbevolen wordt kennis over privacybeleid en –regelgeving onderdeel te maken van het aanbod opleidingen, en het onderwerp privacy bij lijnmanagers in een vaste cyclus onder de aandacht brengen.

4.1.4 Advisering Commissie Persoonsgegevens Amsterdam

De CPA heeft in 2014 omstreeks 35 adviezen (in briefvorm) uitgebracht. Daarnaast zijn ruim tien adviezen vastgelegd in notulen. Een aantal onderwerpen is terug-kerend, waaronder de drie decentralisaties in het sociaal domein en dan met name het RIS-systeem. Tevens heeft de CPA geadviseerd over de privacyprotocollen (zie paragraaf 4.2.2) en de samenwerkings- en inkoopovereenkomsten. Er zijn dertien adviezen gegeven over incidentele leveringen van persoonsgegevens uit de BRP, waarvan tien door de ambtelijk secretaris van een preadvies waren voorzien. De CPA heeft adviezen uitgebracht over zeven transparantiedocumenten op basis waarvan persoonsgegevens door de rve Basisinformatie uit de BRP mogen worden (door-) geleverd.[247]

Wbp Monitor

In opdracht van de CPA heeft ACAM vóór de reorganisatie aan de privacy-coördinatoren een overzicht gevraagd van de verwerkingen van persoonsgegevens binnen de organisatieonderdelen. ACAM heeft gevraagd hierbij te vermelden bij welke afdeling binnen een cluster de verwerking na de reorganisatie zal worden ondergebracht. Per verwerking is een aantal kenmerken gevraagd, bijvoorbeeld of deze gemeld is bij het CBP, of er sprake is van een bewerker en een bewerkers-overeenkomst en of een webapplicatie wordt gebruikt. Ook is gevraagd om de verwachte knelpunten te signaleren. Dit heeft geleid tot de eindrapportage 'Wbp monitor 2014' die aan de stedelijk directeuren is verzonden.[248] Voor de Wbp monitor 2015 zijn dezelfde stappen genomen en is tevens aan de organisatieonderdelen gevraagd of zij (1) bijzondere persoonsgegevens verwerken, (2) bewerkersovereen-komsten hebben afgesloten met de buiten gemeentelijke bewerkers, (3) opvolging hebben gegeven aan de adviezen van de CPA, en (4) de risicoanalyses hebben uitgevoerd.[249]

[247] Jaarverslag 2014; Commissie Persoonsgegevens Amsterdam

[248] Jaarverslag 2014; Commissie Persoonsgegevens Amsterdam

[249] Wbp monitor 2015, 11 januari 2016

In totaal waren er in 2015 227 gegevensverwerkingen (193 in 2014). 44% van 227 van deze verwerkingen is gemeld bij het CBP, waarvan 16 meldingen up-to-date waren.

Het beeld in zowel 2014 als 2015 is dat het overzicht van gemeentelijke processen waarbij persoonsgegevens worden verwerkt niet compleet is. Uit de eindrapportage van de Wbp monitor 2014 en 2015 volgt verder[250]:

1. dat het voorkomt dat een verwerking naar een andere afdeling, cluster of van bestuurscommissie naar een ander organisatieonderdeel wordt verplaatst of dat een proces wordt opgeknipt. Dit kan een extra risico vormen voor de privacy-bescherming.
2. dat meldingen bij het CBP dienovereenkomstig moeten worden aangepast.
3. dat in veel gevallen een actuele en adequate bewerkersovereenkomst voor verwerkingen door partijen buiten de gemeentelijke organisatie (bijvoorbeeld leveranciers) ontbreekt. In 2015 is minder dan de helft van de gevallen een bewerkersovereenkomst afgesloten. In ongeveer 60% van de gevallen moet deze worden geactualiseerd.
4. De bewerkerscontracten zijn over het algemeen nog niet aangepast aan de eisen uit de 'Richtsnoeren voor beveiliging van persoonsgegevens' van het CBP of ontbreken geheel. Dit vormt een risico voor de informatieveiligheid van persoonsgegevens van burgers. In 2015 moet bij ongeveer 60% van de gevallen de bewerkersovereenkomsten worden geactualiseerd.
5. Bij de 23 adviezen van de CPA die zijn uitgevraagd wordt aangegeven dat 20 adviezen zijn opgevolgd. Bij 3 adviezen is, met redenen omkleed, het advies van de CPA niet opgevolgd.

4.1.5 Meldingen incidenten, klachten en datalekken

Incidentenmeldingen

De meeste incidenten komen doordat er te veel of onnodige informatie wordt verzonden via bijvoorbeeld de onbeveiligde mail. Opvallend is dat de incidenten veelal voorkomen bij de instellingen en aanbieders.[251] Dit zijn juist de organisaties waar ze goed op privacy letten, vooral in verband met de vertrouwensrelatie met de cliënt. Soms wordt iets gemeld, maar gaat het om zo weinig informatie dat het bijna geen incident te noemen is. Een eenduidige definitie van een incident ontbreekt. Hierdoor werkt de incidentenrapportage nog niet optimaal. Om deze reden werkt de schouw op dit moment aan het opstellen van een normering om te bepalen wat een incident is.[252]

Meldpunt Datalekken

In het kader van de nieuwe wetgeving voor de meldplicht van datalekken stuurt de gemeente vanuit de rve's een brief naar alle bewerkers van de gemeente. In de brief worden de bewerkers geïnformeerd over wat de gemeente van hen verwacht.

[250] Jaarverslag 2014; Commissie Persoonsgegevens Amsterdam

[251] Interview, 9 november 2015

[252] Interview, 9 november 2015

CIO-Office maakt in overleg met Directie Juridische Zaken (DJZ) het format voor de brief. De gemeente laat daarnaast de organisaties de bewerkersovereenkomsten aanpassen
waarbij aanvullende afspraken worden gemaakt over de te nemen beveiligingsmaatregelen door de bewerker. Er komt ook een nieuw format voor de bewerkersovereenkomst. Dit gebeurt op concernniveau. Zodra deze klaar is wordt deze concernbreed verspreid.[253] Op intranet van Amsterdam worden voorbeelddocumenten geplaatst met o.a. een voorbeeldbrief en een bewerkersovereenkomst.[254]

4.1.6 Concernauditcommissie

In opdracht van de concernauditcommissie (CAC) heeft ACAM een onderzoek uitgevoerd naar in hoeverre de 1ste en 2de lijn de privacycontrol waarborgen zodat aan de Wbp wordt voldaan.

Op basis van het uitgevoerde onderzoek concludeert ACAM in februari 2016: *De opzet van het stelsel heeft nog onvoldoende samenhang en is momenteel van te beperkte kwaliteit om te borgen dat aan de Wbp wordt voldaan. De eerste stappen richting verbetering zijn gezet.*[255]
ACAM geeft daarbij 12 aanbevelingen om het stelsel te verbeteren:[256]

- Actualiseer governance/kaders en beleid en anticipeer op nieuwe wetgeving;
- Pas risicomanagement toe en maak bij voorkeur gebruik van een risicomanagementsysteem;
- Zorg voor een dekkend stelsel van maatregelen om de privacy-risico's te managen;
- Richt monitoring/toetsing in ten aanzien van het naleven van (beleids) kaders, richtlijnen en (wets)regels;
- Gebruik de CPA niet als 2de lijns toezichthouder;
- Installeer en implementeer spoedig de functie van Cluster Privacy Officer conform het IV-functiehuis;
- Verhelder en communiceer de specifieke rol van de Cluster Privacy Officer in de organisatie;
- Beschrijf en borg processen, zoals het meldingsproces;
- Verhelder en communiceer naar de 1ste lijn de specifieke rol van 1ste en 2de lijns juridisch privacy advies en borg de rol van DJZ voor privacy in procesbeschrijvingen in zowel de 1ste als 2de lijn;
- Faciliteer en borg actief het verkrijgen van juridische privacy-kennis;
- Borg de volledigheid en juistheid van bewerkersovereenkomsten;
- Inventariseer alle verwerkingen. Bepaal de privacy-risico's en implementeer maatregelen.

4.1.7 College kondigt maatregelen aan voor naleving privacyregels

Halverwege januari 2016 heeft het college aangegeven vijf maatregelen prioriteiten te geven om de informatiebeveiliging te borgen en om de privacyregels uit de Wet

[253] Interview, 12 december 2015.
[254] Brief Inwerkingtreding meldplicht datalekken per 1 januari 2016, 17 december 2015.
[255] ACAM, Rapport privacycontrol 1ste en 2de lijn, 16 februari 2016.
[256] ACAM, Rapport privacycontrol 1ste en 2de lijn, 16 februari 2016.

bescherming persoonsgegevens (Wbp) na te leven. Dit naar aanleiding van het jaarververslag 2014 van de Commissie Persoonsgegevens Amsterdam.[257] Drie van deze maatregelen hebben betrekking op de afspraken binnen de gemeentelijke organisatie. De eerste maatregel betreft het actualiseren van kaders voor het borgen van de taken en verantwoordelijkheden in de nieuwe gemeentelijke organisatie. Dit door de functies, taken en verantwoordelijkheden van de stedelijke directeuren, rve-managers, de cluster Privacy, Informatiebeveiliging en Bedrijfscontinuïteit-coördinatoren (de cluster PIB-ers), CIO en CISO en CPA beter af te bakenen en door hier uitvoering aan te geven. Daarnaast zal ook in het primaire proces gebruik worden gemaakt van een PIA. Ten slotte zal een Information Security System worden geïmplementeerd waarin per proces wordt vastgelegd hoe er wordt omgegaan met de concernkaders en regelgeving voor privacy en informatiebeveiliging. De tweede aankondigde maatregel heeft betrekking op het versterken van het toezicht (control) op de naleving van privacywetgeving. Uitgangspunt is dat de rve's verantwoordelijk zijn voor hun eigen gegevensverwerkingen en de naleving van de privacyregels. De CISO zal periodiek de naleving van privacyregels door de rve's toetsen en zal zich daarbij baseren op de uitkomsten van de toetsingen door de Cluster Advies Team (CAT) en het Stedelijk Advies Team (SAT). Bij de derde maatregel kondigt het college aan te zullen anticiperen op de nieuwe wetgeving en daarbij de ontwikkelingen met betrekking tot de Europese privacyverordening nauwlettend in de gaten te zullen houden. Tevens zegt het college toe prioriteit te geven aan de Wet meldplicht datalekken.

4.1.8 Conclusie

Privacycoördinatoren hebben een prominente rol als het gaat om borging van privacy binnen het cluster en de rve. Uit de praktijk blijkt dat zij deze rol nog niet volledig kunnen waarmaken. Oorzaken daarvoor zijn dat ze nog niet voor iedereen duidelijk is dat de privacycoördinatoren er zijn, wie ze zijn, en waarvoor men kan aankloppen bij een privacycoördinator. Tot slot was er sprake van een hoge werkdruk en capactiteitsproblemen. Bij Samen DOEN is dit ondervangen door een eigen privacycoördinator aan te stellen. De informatievoorziening eenheid (IVE) van het cluster Sociaal geeft aan dat de werkdruk en capaciteitsproblemen van de privacy-coördinatoren zijn opgelost door middel van inhuur van externe medewerkers. Positief is dat sinds kort een vakoverleg privacy is opgezet waar onder andere de cluster PIB-ers en de CISO samenkomen. Het vakoverleg draagt zorg dat meer concernbrede afstemming over privacyvraagstukken plaatsvindt en privacy-functionissen eenvoudiger te vinden zijn voor de verschillende organisatie-onderdelen.

Positief is dat er in augustus 2014 zowel een Uitgebreide Risico Analyse als een Privacy Impact Assessment is uitgevoerd op de gegevensverwerking van Samen DOEN, OKT en Wijkzorg. Dit heeft geleid tot de implementatie van meerdere beheersmaatregelen. Of er een monitoring plaatsvindt op de implementatie van de beheersmaatregelen en de werking ervan is niet duidelijk. De CPB heeft aangeraden

[257] Commissie Persoonsgegevens Amsterdam, Jaarverslag 2014

voor beveiligingsmaatregelen een reguliere controle en evaluatie in te bedden in het primaire proces. Het lijkt erop dat deze aanbeveling nog niet is overgenomen binnen het cluster Sociaal.

Los van ons onderzoek, maar in lijn met onze bevindingen, concludeert ACAM dat de opzet van het stelsel nog onvoldoende samenhang heeft en van te beperkte kwaliteit is om te borgen dat aan de Wbp wordt voldaan. ACAM constateert verbeteringen.

Het college heeft in januari 2016 aangekondigd de kaders voor het borgen van de taken en de verantwoordelijkheden te zullen actualiseren, het toezicht op de naleving van privacywetgeving te zullen versterken en te zullen anticiperen op nieuwe wetgeving.

Uit de gesprekken komt naar voren dat het nog ontbreekt aan eenduidige definitie voor incidentenmeldingen, waardoor het rapporteren over incidenten nog niet optimaal werkt. De gemeente is bezig met het opstellen van een normering wat als incident kan worden gezien. Ook zijn de transparantiedocumenten voor de cluster Sociaal niet zijn geactualiseerd.

4.2 Afspraken met samenwerkende organisaties

4.2.1 Samenwerkings- inkoop- en bewerkersovereenkomsten

In de afgesloten overeenkomsten van Samen DOEN en OKT wordt aangegeven dat de instellingen zullen werken met het (voorlopige) systeem RIS. Met deze vermelding wordt het registreren in andere systemen, bijvoorbeeld de eigen systemen van de instellingen, niet uitgesloten (zie paragraaf 3.3.2). In diverse gesprekken met de gemeente komt naar voren dat het gebruik van andere registratiesystemen dan RIS en Kidos voor het registeren van persoonsgegevens van cliënten van Samen DOEN en OKT, uit den boze is.[258] Met twee gecontracteerde organisaties van Samen DOEN is overleg geweest over het registeren van cliëntgegevens in RIS en de registratiesystemen van de organisaties.

4.2.2 Privacyprotocollen

De privacyprotocollen van Samen DOEN, OKT of Wijkzorg openen met een preambule. Hierin wordt in het kort weergegeven wat het programma inhoudt en wat de werkwijze is. Deze preambule is tevens bedoeld voor de burgers.[259] Het privacyprotocol is voornamelijk geschreven voor de hulpverleners, met de burger in het achterhoofd.[260] De privacyprotocollen zijn echter niet eenvoudig voor de burger terug te vinden op internet.

[258] Interview, 10 november 2015.

[259] Interview, 10 november 2015.

[260] Interview, 9 november 2015.

Ook de politie, het OM, en andere partners waarmee Samen DOEN, OKT of Wijkzorg hebben samengewerkt, hebben hun eigen privacyprotocollen, die inhoudelijk van elkaar afwijken. Vanwege de afwijkende wettelijke grondslag is het niet mogelijk deze protocollen volledig op elkaar af te stemmen en gelijkluidend te krijgen.[261] Dit geeft in het werkveld allerlei onduidelijkheden hoe te handelen daar waar het gaat om persoonsgegevens.

4.2.3 Werkinstructies

De werkwijzers van Samen DOEN zijn voor de hulpverleners in een systeem te vinden dat binnenkort wordt vervangen. Ook zijn deze werkwijzers te vinden in RIS. Er komt een intranetsite waar ook de afspraken die gemaakt zijn met het forensisch netwerk (netwerk van organisaties die zich richten op de combinatie strafrecht en psychiatrie) en met de schuldhulpverlening worden vermeld.[262] Bij OKT is een dergelijk platform reeds beschikbaar. Informatie die voor OKT van belang is, staat op de website. Informatie die de medewerker kan naslaan om hem/haar te helpen bij het uitvoeren van het werk, zoals een FAQ en de werkwijze, is op de website te vinden.[263] Wijkzorg heeft de beschikbare documentatie geplaatst op de internetsite van de gemeente.

4.2.4 College kondigt maatregelen aan voor naleving privacyregels

Naar aanleiding van het jaarververslag 2014 van de Commissie Persoonsgegevens Amsterdam heeft het college aangegeven vijf maatregelen prioriteiten te geven om de informatiebeveiliging te borgen en om de privacyregels uit de Wet bescherming persoonsgegevens na te leven. Eén van deze maatregelen heeft betrekking op de afspraken met samenwerkende organisaties. Rve's zal worden gevraagd om in 2016 prioriteit te geven aan om te voldoen aan de eisen uit de Wbp ten aanzien van de verplichting tot het sluiten van een bewerkersovereenkomst met externe partijen. Tevens zullen de huidige bewerkersovereenkomsten worden aangepast aan de Wet Meldplicht datalekken.

4.2.5 Conclusie

De gemeente heeft niet vastgelegd in de overeenkomsten met de uitvoerende instellingen dat voor de registratie van persoonsgegevens alleen RIS en Kidos gebruikt mogen worden. Deze afspraken ontbreken. Uit de gesprekken met verschillende functionarissen van de gemeente en de instellingen blijkt dat de gemeente het gebruik van andere systemen niet wil toelaten.
Naast de uitvoerende instellingen van Samen DOEN, OKT en Wijkzorg werkt de gemeente samen met diverse andere instellingen (w.o. de politie, het OM, etc.). Vanwege een andere wettelijke grondslag werken deze partijen met eigen privacy-protocollen die niet altijd aansluiten en op één lijn te krijgen zijn met de protocollen van de gemeente. Gevolg is dat de samenwerkende partners anders omgaan met de

[261] Interview, 10 november 2015.
[262] Interview, 10 november 2015.
[263] Interview, 10 november 2015.

verwerking van (bijzondere) persoonsgegevens en allerlei onduidelijkheden ontstaan. Het college heeft in januari 2016 aangekondigd om de bestaande bewerkersovereenkomsten te actualiseren.

4.3 Afspraken met leverancier geautomatiseerde systemen

Registratie Informatie Systeem (RIS)
In de periode voor de transitie van de jeugdzorg was het programma Om Het Kind (Ouder- en Kindteams) voornemens de informatievoorziening voor het gehele domein (inclusief de zorgaanbieders van de Jeugdzorg) uit te gaan werken. CIO-Office heeft geadviseerd terughoudend te zijn met investeringen in nieuwe (kostbare) systemen gezien de grote veranderingen in het domein van de Jeugdzorg. De rol van de gemeente bij de uitvoering van de Jeugdzorg stond destijds niet vast. Dit heeft het programma Om Het Kind doen besluiten zoveel mogelijk gebruik te maken van de bestaande registratiesystemen (waaronder RIS).[264]

De gemeente is inmiddels gestart met een onderzoek naar de toekomstige informatievoorziening voor Samen DOEN, OKT en Wijkzorg, waarbij zij voornemens is een nieuw registratiesysteem of -systemen te implementeren die de oude RIS-modules gaan vervangen. De uitgangspunten voor het IV-systeem worden samen met de ketenpartners gedefinieerd. Tevens zijn er overleggen gaande met organisaties zoals cliëntenbelang en cliëntenraden. De gesprekken moeten leiden tot een programma van eisen. Een stuurgroep bestaande uit de rve-manager GGD, rve-manager IV cluster Sociaal, afdelingshoofd Zorg (rve OJZ), rve-manager Participatie en de manager IV en innovatie van SIGRA voert regie op het project.

4.3.1 Hoofd- en bewerkersovereenkomst

De gemeente heeft met de leverancier van de RIS-modules van Samen DOEN, OKT en Wijkzorg een hoofdovereenkomst en een bewerkersovereenkomst afgesloten (zie paragraaf 3.4.1). We zullen in deze paragraaf op een aantal onderwerpen terugkomen op basis van de bevindingen uit paragraaf 3.4.1 en onderzoeken welke afspraken zijn uitgevoerd. Daaropvolgend zullen we de analyse van logbestanden, exportmogelijkheden van cliëntgegevens, de uitgevoerde pen- en hacktesten en de autorisaties in RIS bespreken.

Exitplan als een continuïteitsplan
De bedrijfsvoering van de gemeente, c.q. de feitelijke gebruikers, kan in gevaar komen wanneer de leverancier van RIS onverhoopt in de problemen raakt (bijvoorbeeld bij faillissement) of indien de gemeente in de toekomst de dienstverlening door een andere partij wil laten uitvoeren (i.e. exitplan).[265] Het exitplan[266] is tot op heden

[264] Interview, 9 juli 2015

[265] Hoofdovereenkomst tussen Gemeente Amsterdam en [leverancier], 16 april 2015.

[266] Het vastleggen van een exitplan is bedoeld om de aanpak, verplichtingen en voorbereidingen te beschrijven voor een soepele overname door de gemeente of door een door de gemeente aangestelde derde, waarbij de continuïteit van de dienstverlening voorafgaand en gedurende transitie naar de opvolgend leverancier(s) veilig gesteld wordt (bron: Hoofdovereenkomst tussen Gemeente Amsterdam en [leverancier], 16 april 2015).

echter niet opgesteld en de uitwijkingslocatie is nog niet operationeel. De partijen werken momenteel aan een continuïteitsoplossing waarmee de continuïteit ten aanzien van operationeel blijven van RIS en het kunnen doorontwikkelen van RIS niet in gevaar komt, mocht de leverancier in problemen raken.[267] De continuïteitsoplossing houdt in dat de gemeente eigenaar wordt van een backup-server met daarop de data van RIS. Tevens zal via een escrow-regeling, waarin de gemeente wordt beschermd dt bij het wegvallen van de leverancier de broncode veilig wordt gesteld.[268] Zeer recent, 10 februari 2016, heeft de gemeente hiervoor een overeenkomst getekend met de leverancier van de software.[269] De uitwijklocatie is in opbouw en bevindt zich in februari 2016 nog in de realisatiefase.[270] De testfase moet nog plaatsvinden.[271]

NEN-ISO certificaat
Met de leverancier is afgesproken dat zij zich maximaal zal inspannen om binnen zes maanden na de ingangsdatum van de hoofdovereenkomst (16 april 2015) te beschikken over een geldig NEN-ISO/IEC 27001 (managementsysteem voor informatiebeveiliging) certificaat en garandeert binnen negen maanden na ondertekening over het betreffende certificaat te beschikken. [272] Dit certificaat is nog niet beschikbaar. De gemeente geeft aan dat het certificeringstraject veel langer duurt dan eerste instantie werd gedacht.[273]
De leverancier verklaart dat zij voldoet aan de beveiligingsrichtlijnen, zoals opgenomen in de ICT-Beveiligingsrichtlijnen voor webapplicaties[274] met classificatie "midden" en "hoog".[275] In de gesprekken wordt aangegeven dat vanuit de gemeente (functioneel beheer) strakker gestuurd wordt op het behalen van certificering.[276]
De privacycoördinator moet binnen zijn of haar cluster in beeld hebben welke afspraken over informatiebeveiliging en privacy gemaakt zijn met externe partijen en dient daarop te monitoren.[277] De lijn is verantwoordelijk voor het nemen van een besluit. Vanuit de gemeente ontbreekt het aan een strakke sturing op de leverancier, dan wel op het nakomen van eigen afspraken met de leverancier.

Bewaartermijnen
Voor RIS OKT is de bewaartermijn van herleidbare persoonsgegevens ingesteld op 15 jaar nadat de laatste actie in een dossier (aanmaken, bewerken of verwijderen van data) is afgerond. Nadat de bewaartermijn van 15 jaar is verstreken worden de herleidbare persoonsgegevens (NAW, BSN en geboortedatum) automatisch

[267] Hoofdovereenkomst tussen Gemeente Amsterdam en [leverancier], 16 april 2015.
[268] Interview, 26 mei 2015 en mailing, 1 december 2015.
[269] Individuele escrow-overeenkomst voor broncode inzake RIS-modules Gemeente Amsterdam, 12 februari 2016.
[270] De gemeente geeft aan dat technici bezig zijn om de installatie en het werkend te krijgen. De servers zijn inmiddels geplaatst.
[271] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016..
[272] Hoofdovereenkomst tussen Gemeente Amsterdam en softwareleverancier., 16 april 2015.
[273] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[274] deel 1 en 2, januari 2012 van het Nationaal Cyber Security Centrum.
[275] Interview, 26 mei 2015 en mailing, 1 december 2015.
[276] Interview, 8 december 2015.
[277] Interview, 12 december 2015.

geanonimiseerd. In RIS Samen DOEN en RIS-Wijkzorg bestaat eenzelfde functie voor de bewaartermijn, echter is deze niet actief ingesteld op een bepaalde termijn. Deze anonimisering na de bewaartermijn zal na afstemming met de opdrachtgevers van Wijkzorg en Samen Doen ook hier ingeregeld worden.[278]

Analyse logbestanden
Het logsysteem van de gemeente waarmee kan worden teruggezien wie al dan niet onrechtmatig inlogt of bewerkingen maakt in de RIS-modules. In de praktijk wordt er door de leverancier van RIS op drie niveaus gelogd (i.e. audit trial)[279]:

1. Access log: op basis van het IP-adres wordt geregistreerd op welk tijdstip werd ingelogd en hoe vaak de toegang is geweigerd op basis van een onjuist wachtwoord. Deze log is alleen toegankelijk voor de leverancier. De leverancier analyseert meerdere malen per dag het logbestand om te zien of er onrechtmatig is ingelogd. Bijzonderheden worden doorgegeven aan functioneel beheer, zodat deze actie kan ondernemen.[280]
2. Log van alle SQL-queries op de RIS-modules: deze log is toegankelijk voor de leverancier en wordt niet geanalyseerd. In de log is te zien of er exportbestanden zijn aangemaakt en door wie.
3. Log van cliëntdossiers: hierin is informatie opgenomen over welke gebruiker welke handelingen wanneer heeft gedaan in het cliëntdossier (m.a.w. registratie, mutatie en raadplegen van gegevens). De gebruiker die toegang heeft tot een dossier kan de log bekijken. Sinds halverwege 2015 is de loggingfunctie ook raadpleegbaar voor functioneel beheer.[281] Deze loggingfunctie maakt een analyse op onrechtmatig gebruik mogelijk.[282] Een totale analyse van de logginsgegevens is uitgevoerd bij de pen- en hacktest van 2015 over de periode 2014-2015. De gemeente acht het niet nodig de loggegevens structureel te analyseren, omdat de klanthouders zelf logs kunnen bekijken.[283]

[278] Feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016.
[279] Interview, 26 mei 2015 en mailing, 1 december 2015.
[280] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016
[281] Stedelijk directeur sociaal, feitelijk wederhoor, , 15 februari 2016.
[282] Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy; Cluster sociaal IV systeem RIS 3D's, versie 1.2, 28 augustus 2014.
[283] Als er twijfel is over totstandkoming of bewerking van een specifiek dossier, kan functioneel beheer de logging in het betreffende dossier inzien, zodat bekeken kan worden welke medewerkers aan het dossier gewerkt hebben. Bron: Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016

Export mogelijkheden
De export mogelijkheden van gegevens uit RIS variëren per RIS-module en zijn als volgt:

Tabel 4.1 – Exportmogelijkheden per RIS-module

RIS-module	Mogelijkheden
RIS Samen DOEN	Verschillende persoonsgegevens van de cliënten kunnen worden geëxporteerd, zoals: naam, adres, woonplaats, geboortedatum, geslacht, BSN en integratietrede van cliënten. Functioneel beheer maakt op basis van de totale export maandrapportages.
RIS Ouder- en Kindteams	Er zijn drie op maat gemaakte exports. Het is niet mogelijk voor de gemeente om alle gegevens te exporteren. OKT gebruikt de exports om het in een ander systeem in te lezen en management rapportages te genereren.
RIS Wijkzorg	Er zijn een aantal op maat gemaakte exports Het is niet mogelijk voor de gemeente om alle gegevens van de cliënten te exporteren. Wijkzorg heeft drie keer een totale export van de bestanden aan de leverancier gevraagd voor het opstellen van een rapportage.

De tabel laat zien dat er tussen de RIS-modules duidelijke verschillen zijn in wat voor gegevens er geëxporteerd worden. De exports van RIS Samen DOEN bevatten veel persoonsgegevens, waarbij de vraag gesteld kan worden of deze daadwerkelijk noodzakelijk zijn. Functioneel beheer gebruikt de namen niet bij het vervaardigen van managementrapportages, maar hebben wel de postcodes nodig om de indeling naar wijken te maken. Op grond daarvan worden geanonimiseerde rapportages gemaakt.

Veilig mailen
Naast deze wijze van informatievoorziening, wordt ook gebruik gemaakt van gegevensuitwisseling via onbeveiligde e-mail kanalen. De gemeente beschikt nog niet over beveiligde kanalen. Ook bij de instellingen gaat gegevensuitwisseling geregeld over onbeveiligde kanalen.[284] Het hele ICT platform moet daar voor nog ingericht worden. Het Amsterdamse domein is volgens DICT onveilig om intern te mailen.[285] Samen DOEN is bezig met een beveiligde mail omgeving (zorgmail) te creëren. De gemeente heeft de verwachting uitgesproken deze in maart 2016 gerealiseerd is.[286]

Penetratie- en hacktest
In mei/juni 2014 is er door een extern bureau een penetratie- en hacktest uitgevoerd op alle RIS-modules. De gemeente geeft aan dat de fysieke zaken die daaruit

[284] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[285] Interview, 10 november 2015.
[286] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.

voortkwamen direct zijn verholpen door de leverancier van RIS. Met de organisatorische zaken is de gemeente bezig. Een encryptie moet nog worden gerealiseerd. De VPN-verbinding is sinds februari 2015 actief geworden voor de RIS-modules.[287] Qua autorisatie moet er ook nog een aantal zaken gebeuren, voornamelijk bij het uit dienst treden van gebruikers; dit is nog niet overal goed geregeld.[288] Wel vervalt het wachtwoord elke 60 dagen en moet deze dan gewijzigd worden. Zodra 180 dagen geen gebruik wordt gemaakt van RIS, vervallen de rollen en heeft de gebruiker geen rechten meer in RIS. Bij Samen DOEN geven de teamassistenten een uitdiensttreding door aan de programmasecretaris, die vervolgens de autorisatie voor RIS intrekt.[289]

In de periode september tot en met oktober 2015 is wederom een pen- en hacktest uitgevoerd op de RIS-modules. Het betrof een zogenaamde grey-box test, waarbij een aantal randvoorwaarden zijn geschapen door de gemeente en de softwareleverancier om de pen- en hacktest meer waarde te geven, zoals het verlagen van de beveiliging en het geven van toegang tot de webapplicaties.[290] In november 2015 is een hertest uitgevoerd. Hierbij zijn geen beveiligingsproblemen geconstateerd.[291] Volgens het Cluster Sociaal heeft de CISO alert gereageerd op het geconstateerde beveiligings-probleem bij RIS. CISO is direct door het cluster ingelicht en er zijn acties uitgezet richting de leverancier.[292]

Autorisaties RIS
In paragraaf 3.4.1 is beschreven hoe de autorisaties in opzet zijn geregeld. Hier zullen we, met behulp van de door de softwareleverancier beschikbaar gestelde data, analyseren hoe de autorisaties in de praktijk zijn vormgegeven. De uitkomsten van de analyse is in de onderstaande tabellen weergegeven. De onderstaande tabel geeft een indicatie van het aantal medewerkers van Samen DOEN, OKT en Wijkzorg die toegang hebben tot meerdere RIS-modules.

Tabel 4.2 – Aantal gebruikers die toegang hebben tot meerdere modules binnen Samen DOEN, OKT en Wijkzorg[293]

Aantal modules waartoe toegang is verleend	Aantal gebruikers
1	2.103
2	47
3	3
Totaal	2.153

[287] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[288] Interview, 26 mei 2015 en mailing, 1 december 2015.
[289] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[290] Plan van aanpak, bevindingen n.a.v. hack- en pentest en her-test, 4 november 2015.
[291] Interview, 30 november 2015.
[292] Memo beveiliging RIS, 16 november 2015.
[293] Data uit mailing , 30 april 2015.

Een aantal medewerkers van Samen DOEN, OKT en Wijkzorg hebben toegang tot twee of drie RIS-modules. Functioneel beheer geeft aan dat dit met name om psychologen gaat die zowel voor Samen DOEN en OKT werken. Zij moeten in beide modules kunnen, zodat zij cliënten kunnen bedienen in verschillende werkgebieden.[294] In paragraaf 3.4.1 is geconstateerd dat klanthouders andere gebruikers toegang kunnen verlenen tot een cliëntdossier. Het aantal gebruikers waaraan toegang tot een dossier kan worden verleend is niet gemaximaliseerd.[295] De leverancier van de RIS-modules geeft aan dat in de praktijk dit per dossier kan oplopen tot zo'n 11 gebruikers die toegang hebben gekregen tot een dossier. Hier wordt geen toezicht op gehouden, behalve door eventueel de klanthouder zelf. Uit de gesprekken blijkt dat de functioneel beheerder van de gemeente mogelijk ook toegang heeft tot zorginhoudelijke gegevens van de cliënten.[296] Volgens OKT kwamen gegevens naar buiten waar de gemeente geen toegang toe behoorde te hebben.[297]

4.3.2 Conclusie

Veel van de afspraken die in de hoofd- en bewerkersovereenkomst met de leverancier nog nader uitgewerkt hadden moeten worden, zijn niet uitgewerkt. De gemeente stelt dat de softwareleveranciers qua beveiliging moeten voldoen aan ISO normeringen en een adequate beveiliging voor webapplicaties conform criteria van het Open Web Application Security Project (OWASP).

De privacycoördinator moet binnen zijn of haar cluster in beeld hebben welke afspraken gemaakt zijn met externe partijen als het gaat om informatiebeveiliging en privacy en dient daarop te monitoren. De sturing op het nakomen van de afspraken met de leverancier is nog niet optimaal. Zo beschikt de softwareleverancier nog niet over de vereiste ISO certificering en ontbreekt het exitplan waarin is opgenomen op welke wijze er, ten einde van de overeenkomst met de leverancier, overdracht naar een andere dienstverlener plaatst kan vinden. Hierdoor kan de continuïteit van de hulpverlening gevaar lopen. Positief is dat continueringsoplossingen in ontwikkeling zijn en dat de gemeente zeer recent een escrow-overeenkomst getekend heeft met de softwareleverancier. Hierdoor zijn stappen gezet om de continuïteit te waarborgen ten aanzien van operationeel blijven van het registratiesysteem.

Bij Samen DOEN hebben een aantal functionarissen de mogelijkheid om bepaalde persoonsgegevens van cliënten te exporteren die voor haar doel niet noodzakelijk zijn. Daarmee is het risico voor privacyschending aanwezig.

Duidelijk is geworden dat gegevens zowel bij de gemeente als bij instellingen soms via e-mail worden verzonden. Bij de gemeente gebeurt het over onbeveiligde kanalen. Ook bij de instellingen gaat gegevensuitwisseling geregeld onbeveiligd. In beide

---

[294] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.

[295] Mail, 19 februari 2016.

[296] Per 17 februari 2016 zijn er 5 accounts voor de functioneel beheerders voor het registratiesysteem Samen DOEN (bron: mail, 17 februari 2016).

[297] Interview, 10 november 2015.

gevallen is het niet de bedoeling gegevens via deze kanalen uit te wisselen (norm 4). Ook zijn de bewaartermijnen bij RIS Samen DOEN en RIS Wijkzorg nog niet geautomatiseerd.

Meerdere medewerkers van Samen DOEN, OKT en Wijkzorg hebben in RIS toegang tot informatie van meerdere wijkteams en/of RIS modules. De gemeente geeft aan dat dit voornamelijk om jeugdpsychologen gaat. Door de mogelijkheid om als klant-houder meerdere hulpverleners toegang te verlenen tot een dossier is het risico aanwezig dat medewerkers inzage krijgen in privacygevoelige gegevens van cliënten die niet vanuit hun taakuitoefening noodzakelijk zijn.

Loggingfunctionaliteiten zijn voor de gemeente volop beschikbaar, maar analyse op loggingdata op onrechtmatigheden bij inzage of mutaties in cliëntdossiers vindt vooralsnog niet actief plaats.

4.4 Afspraken voor een lerende organisatie

In verschillende documentatie van de gemeente, zoals de uitgebreide risicoanalyse op de drie decentralisaties en het gebruik van de RIS-modules, wordt onderschreven dat goede training en opleiding voor het gebruik van de registratiesystemen en aan-vullende bewustwording noodzakelijk is om eventuele fouten te voorkomen.[298] In deze paragraaf laten we zien hoe de lerende organisatie in de praktijk is ingevuld.

4.4.1 Concernbreed

Uit de gesprekken kwam naar voren dat er nog geen concernbrede opleiding over privacy is.[299] De eerder ontwikkelde cursus risicoanalyse (zie paragraaf 3.5.2), waar privacy in beperkte mate aan bod komt, zal in het eerste kwartaal van 2016 voor de derde keer gehouden worden.[300] Deelnemers aan de cursus zijn vaak projectleiders, informatiemanagers, etc.[301]
In oktober 2015 is er studiedag georganiseerd over de nieuwe Europese privacyverordening. Deze studiedag had als doel kennisverkrijging en –deling tussen de ambtelijke privacyfunctionarissen van het cluster Sociaal en andere clusters.[302]

De CIO-Office heeft het voornemen een concernbrede campagne te initiëren om privacy onder de aandacht te brengen.[303] Dit zal in samenwerking gaan met Bureau Integriteit en Communicatie. Dit initiatief komt voort uit het implementatieplan BIG waarin is aangegeven dat centraal activiteiten worden gestart om de bewustwording van de Amsterdamse ambtenaren op het gebied van informatiebeveiliging te

[298] Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy; Cluster sociaal IV systeem RIS 3D's, versie 1.2, 28 augustus 2014.
[299] Interview, 8 december 2015.
[300] Interview, 12 december 2015.
[301] Interview, 12 december 2015.
[302] Stedelijk directeur sociaal, feitelijk wederhoor,, 15 februari 2016.
[303] Interview, 9 juli 2015.

verhogen. Het verhogen van de aandacht voor informatiebeveiliging en ook privacy zijn eisen die vanuit de BIG en ook de Wet Structuur uitvoeringsorganisatie werk en inkomen (wet SUWI) worden verplicht. Door centraal de clusters en de rve's te ondersteunen geeft Amsterdam invulling aan deze verplichtingen en wordt de implementatie van de BIG op cluster en rve-niveau ondersteund.[304] Voor de campagne zal een aparte projectleider worden aangetrokken. Voor het dynamische deel van de campagne zal gedurende 2015-2016 een 'minicompetitie' worden gestart voor het privacybewustzijn van informatiebeveiliging en privacy, bestaande uit E-learning voor de gehele stad, speciale modules voor directies, managers, beheer-afdelingen en andere specifieke doelgroepen waarbij aandacht is voor Privacy en de BIG.[305] De campagne zal uitgevoerd worden in samenwerking met de leverancier. De intentie is van het onderwerp bewustwording een continue activiteit te maken dat zoveel mogelijk gaat aansluiten op lopende activiteiten van de organisatie, zoals bestaande opleidingen en reeds geplande activiteiten.[306] De plannen zijn nog in conceptfase.

Het voordeel van een concernbrede opleiding wordt niet bij alle functionarissen in de organisatie gedragen. Enerzijds ziet men het voordeel om op stedelijk niveau een stedelijke boodschap uit te dragen.[307] Anderzijds wordt het risico benoemd dat de training niet specifiek afgestemd is op de jeugdhulp.[308] Een functionaris van de gemeente stelde voor de concernbrede gesprekken te laten gaan over hoe privacy is ingevuld binnen de verschillende organisatieonderdelen. Hier kunnen namelijk verschillende culturen zijn ontstaan als het gaat om privacybewustzijn.[309]

4.4.2 Cluster Sociaal

In de voortgangsrapportage risicomanagement sociaal domein wordt als risico onderkend dat de regels omtrent privacy onvoldoende worden nageleefd. Om dit te ondervangen wordt o.a. als maatregel voorgesteld om de kennis over privacybeleid en –regelgeving onderdeel te maken van het aanbod van opleidingen. [310]

Leerlijn

De inhoudelijke modules van de leerlijn van Samen DOEN vormen een basisset aan kennis en vaardigheden voor de professionals in de teams. Het gaat hier onder andere om de modules waar ingegaan wordt op de werkwijze, RIS, ZRM, herkennen van kindermishandeling, licht verstandelijke beperking en GGZ-problematiek.[311] In de uniforme werkwijze van Samen DOEN wordt aangegeven dat de medewerkers

[304] Campagne Bewustwording Informatiebeveiliging & Privacy 2015/2016, 14 juni 2015.
[305] Campagne Bewustwording Informatiebeveiliging & Privacy 2015/2016, 14 juni 2015.
[306] Campagne Bewustwording Informatiebeveiliging & Privacy 2015/2016, 14 juni 2015.
[307] Interview, 8 december 2015; Interview, 10 november 2015.
[308] Interview, 8 december 2015.
[309] Interview, 10 november 2015.
[310] Voortgangsrapportage risicomanagement sociaal domein: Voortgang en risico's van de decentralisaties Jeugdwet, AWBZ/Wmo, Participatiewet, de samenhang tussen de drie decentralisaties (3D), Samen DOEN en Dragende samenleving, oktober 2014, blz. 78.
[311] Visie op leren en ontwikkelen: De Samen DOEN in de buurt leerlijn, juli 2013.

getraind zijn in de uniforme werkwijze, waarin nadrukkelijk het aspect privacy aan de orde komt.[312]
Nieuwe medewerkers bij Samen DOEN krijgen vanuit de leerlijn diverse (verplichte) basismodules aangeboden. Ook kunnen medewerkers zich inschrijven voor verschillende verdiepingsmodules.[313] Samen DOEN wil dat het privacyprotocol in het inwerkprogramma wordt geborgd. Dit gebeurt in het huidige inwerkprogramma onvoldoende.[314]
De leerlijn van Samen DOEN bevat echter op het moment van schrijven geen module waar expliciet aandacht wordt geschonken aan privacy van cliënten. De gemeente is in overleg met een externe partij die dit gaat ontwikkelen. Wel komt het onderwerp privacy ter sprake in de 'winterschool', waarbij een groot aantal modules en trainingen te volgen zijn. De verwachting is dat na de winterschool de privacy module wordt geïntegreerd in de basismodules van Samen DOEN. In deze module gaat geen privacygevoelige informatie gedeeld worden.
In de interviews kwam ter sprake dat aanvulling op de leerlijn kan zijn om vanuit de teams zelf een inwerktraject voor nieuwe collega's te initiëren. Een nieuwe collega leest de protocollen en uniforme werkwijzen, maar deze worden pas echt concreet als door een collega verteld wordt hoe er binnen Samen DOEN gewerkt wordt.[315]

OKT heeft een workshop die ingaat op privacy. Deze is in de periode van mei tot en met december 2015 zeven keer gegeven op basis van open inschrijving.[316] Ook zijn er vier workshops aan teams gegeven. Daarnaast is in de bijeenkomsten voor nieuwe medewerkers, die vrijwel elke maand gegeven worden, aandacht besteed aan de hoofdlijnen van het privacybeleid.[317]
In de workshop privacy gaat het niet alleen om privacy, maar ook hoe je als hulpverlener omgaat met datgene wat een ouder vertelt. Wat is in zo'n situatie van belang? Wat is de eigen verantwoordelijkheid en die van de ouder? Wanneer kun je daaraan voorbijgaan? In de workshop worden instrumenten meegegeven, zoals een afwegingskader voor privacy. Hier gaat het om welke vragen een hulpverlener kan stellen voordat hij of zij de privacy van de klant schendt. Dit geldt met name als veiligheid in het geding komt. Hieruit volgt een keuze, welke vervolgens gemotiveerd en gedocumenteerd moet worden. De hulpverlener moet zich dan nog altijd afvragen welke gegevens gedeeld moeten worden. Dit zou altijd het minimale moeten zijn.[318]

[312] Uniforme Werkwijze Samen DOEN in de buurt versie januari 2015, blz. 10.
[313] Interview, 26 oktober 2015.
[314] Interview, 10 november 2015.
[315] Interview, 26 oktober 2015.
[316] Per keer waren ongeveer 15 medewerkers aanwezig. Dit waren Ouder- en kindadviseurs, jeugdverpleegkundigen, jeugdspsychologen, jeugdartsen en teamleiders (bron: Feitelijk wederhoor, stedelijk directeur sociaal, 15 februari 2016).
[317] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.
[318] Interview, 10 november 2015.

Ten behoeve van de leerlijn Wijkzorg zijn er de afgelopen maanden zowel RIS-trainingen als ZRM-trainingen georganiseerd voor professionals. De gemeente geeft aan dat begin 2016 vanuit de gemeente begonnen wordt met een basistraining Wijkzorg. De al lopende trainingen voor RIS en ZRM worden daar een verdieping van. Deelname aan de basistraining is vrijwillig. In de training is privacy geen apart onderdeel, maar komt wel zijdelings langs.[319]

Aanspreekpunten en aandachtsfunctionarissen
In januari 2016 gaat de privacycoördinator van Samen DOEN en een aandachts-functionaris in een zogenaamde Roadshow bij de wijkteams langs om het nieuwe privacyprotocol te presenteren. De presentatie heeft als doel een toelichting te gegeven op het privacyprotocol en tegelijkertijd het privacybewustzijn een boost te geven.
De implementatie van privacybeleid vanuit het programmateam naar de praktijk wordt binnen Samen DOEN als een grote uitdaging gezien. Het proces van terug-koppelen verloopt als volgt. Er wordt beleid gevoerd en dit wordt besproken in het overleg met teamleiders en in het programmateamoverleg. Vervolgens verspreidt de privacycoördinator van Samen DOEN de aanpassingen naar de teamassistenten met de vermelding dat de aanpassingen besproken moeten worden in hun teams. Hierbij wordt vermeld dat de bijhorende documentatie te vinden is op intranet. Vaak gebeurt het nog dat als er een afspraak is gemaakt, bijvoorbeeld over veilig mailen, het uiteindelijk blijkt dat weinig medewerkers zich houden aan de afsrpraak. De enige uitweg die men binnen Samen DOEN dan ziet is de afspraken te blijven herhalen. Ook de aandachtsfunctionarissen worden betrokken bij het terugkoppelen. Zij kunnen informatie doorzetten naar de overige teamleden. Er zijn vier aandachts-functionarissen privacy, waarvan drie er recent zijn bijgekomen. Met de vier aandachtsfunctionarissen worden nu alle wijkteams van Samen DOEN gedekt.[320]
De juridische werkgroep privacy Samen DOEN vergadert iedere maand. In de werkgroep worden privacyvraagstukken besproken die zich in de praktijk voor doen. In de werkgroep wordt gezamenlijk naar oplossingen gezocht. De PIB'ers van IVE Sociaal zijn geen onderdeel van de werkgroep.[321]

Privacyschouw Jeugd
In de nulmeting van de privacyschouw Jeugd zijn op hoofdlijnen geen grote omissies in de omgang met privacy geconstateerd.[322] Wel is er een lijst met verbeteracties uit voortgekomen. Deze eerste maatregel betreft punten waarop een hogere mate van zorgvuldigheid kan worden bereikt, zaken wat meer formeel worden afgehecht en structurele ingrepen die het functioneren van professionals en transparantie van het nieuwe jeugdstelsel bevorderen.[323] De belangrijkste bevindingen zijn hieronder schematisch weergegeven.

[319] Interview, 10 november 2015.
[320] Mail, 14 december 2015
[321] Interview, 26 oktober 2015..
[322] Rapport Nulmeting Privacyschouw Jeugd Amsterdam, september 2015.
[323] Rapport Nulmeting Privacyschouw Jeugd Amsterdam, september 2015.

Tabel 4.4 – Bevindingen privacyschouw Jeugd

Bevinding	Actie	Status
Structurele aandacht privacy	Jaarlijks/periodiek schouwen	Wordt onderdeel van advies bij de eindrapportage conform de wens van het college
Bewustzijn bij functionarissen	Incidentenrapportage helpt bij bewustwording. Verdere acties nog vaststellen	In ontwikkeling
Vaststellen privacyprotocollen	Vaststellen door alle betrokken partijen	Uitgevoerd
Communicatie burgers/procedure inzage, wijzigen dossier	Nog vaststellen	Niet uitgevoerd, bestempeld als belangrijk
Handelingsvrijheid voor professionals	Mogelijke interventies zijn geformuleerd	Gekozen interventie moet nog worden vastgesteld
Onduidelijkheid rondom verantwoordelijkheid privacy	Simulatiemiddag met verschillende partijen om verantwoordelijkheden helder te krijgen	Is gepland

Een tweede maatregel die is genomen naar aanleiding van de schouw is een simulatiemiddag met verschillende betrokken partijen om samen de bestuurlijke en ambtelijke verantwoordelijkheden scherp te krijgen. In februari 2016 lopen fase 2 en 3 van de privacyschouw Jeugd. Naar verwachting is eind maart 2016 een concept rapportage van het externe onderzoeksbureau opgeleverd (3e fase van de privacyschouw) en zal het college de privacyschouw Jeugd eind april 2016 agenderen en vaststellen.[324]

4.4.3 College kondigt maatregelen aan voor naleving privacyregels

Halverwege januari 2016 heeft het college aangegeven vijf maatregelen prioriteit te geven om de informatiebeveiliging te borgen en om de privacyregels uit de Wet bescherming persoonsgegevens na te leven. Dit naar aanleiding van het jaarververslag 2014 van de Commissie Persoonsgegevens Amsterdam.[325] Eén van deze maatregelen heeft betrekking op de afspraken voor een lerende organisatie. In 2016 zal worden ingezet op het vergroten van het bewustzijn over informatie-beveiliging en privacy bij de medewerkers. Hiertoe zal door de CIO in het eerste kwartaal 2016 een campagne worden georganiseerd waarbij aandacht zal worden besteed aan privacy en informatiebeveiliging. Verder zal de CIO begin 2016 extra aandacht besteden aan informatie deling in de ketens en de borging van de privacy daarbij.

[324] Stedelijk directeur sociaal, feitelijk wederhoor, 15 februari 2016.

[325] Commissie Persoonsgegevens Amsterdam, Jaarverslag 2014, 2014.

4.4.4 Conclusie

Vanuit de gemeente is er over het algemeen gezien nog weinig concreetheid over de opleidingen en training voor privacy(bewustzijn), terwijl diverse rapportages een duidelijke noodzaak aankaarten dat deze er moeten komen. Op concernniveau heeft zich dit tot op heden enkel nog geuit door een cursus risicoanalyse, een incidentele studiedag en het ontwikkelen van plannen om privacybewustzijn te stimuleren middels onder andere E-learning en speciale modules. Het blijft vooralsnog bij voornemens die al lang bestaan. Het nut van concernbrede opleidingen wordt niet overal in de organisatie gedragen vanwege de verschillen in de specifieke werkterreinen waar geopereerd wordt.

Binnen het cluster Sociaal vinden er wel deelopleidingen plaats, maar in de meeste gevallen zijn deze niet nadrukkelijk gericht op privacy. Toch zijn op dit vlak enkele bewegingen te zien. Zo heeft OKT de eerste stappen gezet door geregeld privacy workshops te organiseren. De hulpverleners krijgen hier ook instrumenten mee, zoals een afwegingskader bij privacy. Samen DOEN wil dit jaar privacy als vast onderdeel opnemen in de leerlijn. Dit werd tot op heden voornamelijk onder de aandacht gebracht door de privacycoördinator en aandachtsfunctionarissen privacy van Samen DOEN. Wijkzorg heeft nog geen concrete plannen om privacy op te nemen in de leerlijn.

Privacyschouw Jeugd is een goed instrument om privacy binnen Samen DOEN, OKT en Wijkzorg onder de aandacht te brengen. Bovendien heeft het geleid tot de implementatie van meerdere beheersmaatregelen. De schouw is echter wel eenmalig en zou een cyclisch karakter moeten krijgen.

De lerende organisatie lijkt gestalte te krijgen, maar het is nog erg beperkt en niet echt in de organisatie verankerd. De belangrijkste vraagbaken voor de hulpverleners voor privacy blijkt de casuïstiekoverleggen te zijn. Deze overleggen zijn casusgericht, en privacy komt hierin incidenteel naar voren als gespreksonderwerp, op initiatief van de professional zelf. Het college heeft in januari 2016 aangekondigd om het bewustzijn over privacy bij de medewerkers te zullen vergroten.

4.5 Conclusie

De uitvoering van deze organisatorische afspraken (onderzoeksvraag drie) toetsen wij aan de normen uit de Wbp en aan de normen die het ambtelijk apparaat zich zelf aanvullend heeft opgelegd.

De privacycoördinatoren van cluster Sociaal hebben een prominente rol als het gaat om borging van privacy. Helaas blijken zij deze rol nog niet volledig te kunnen waarmaken doordat zij moeilijk in de organisatie te vinden zijn of onduidelijkheid in de organisatie bestaat waarvoor men bij hen kan aankloppen. Bij Samen DOEN is dit enigszins ondervangen door een eigen privacycoördinator aan te stellen. De werkdruk en capaciteitsproblemen binnen de IVE Sociaal, die zich tot december 2015 voordeden, lijken onlangs ondervangen te zijn met inhuur van externe medewerkers.

Het sinds kort opgezette vakoverleg Privacy, waar onder andere de cluster PIB-ers en de CISO samenkomen, draagt zorg dat meer concernbrede afstemming over privacy-vraagstukken plaatsvindt en dat de privacyfunctionarissen eenvoudiger zijn te vinden voor de verschillende organisatieonderdelen.

Positief is dat er in 2014 zowel een URA als een PIA is uitgevoerd op de gegevens-verwerking van Samen DOEN, OKT en Wijkzorg. Dit heeft geleid tot de implementatie van meerdere beheersmaatregelen (norm 4). Of er een monitoring plaatsvindt op de implementatie van de beheersmaatregelen en de werking ervan is niet duidelijk. De CPB heeft aangeraden voor beveiligingsmaatregelen een reguliere controle en evaluatie in te bedden in het primaire proces. Het lijkt erop dat deze aanbeveling nog niet is overgenomen binnen het cluster Sociaal.
De transparantiedocumenten, die gebruikt worden voor het verkrijgen van BRP-gegevens bij de cluster Sociaal, zijn niet volledig geactualiseerd.

De gemeente heeft niet vastgelegd in de overeenkomsten met de uitvoerende instellingen dat voor de registratie van persoonsgegevens alleen RIS (en Kidos) gebruikt mag worden. Dit sluit niet aan met wat de gemeente zelf voor ogen heeft. De gemeente werkt samen met andere dan de uitvoerende instellingen, zoals de politie, OM etc. Deze gebruiken andere privacyprotocollen die niet altijd aansluiten bij die van de gemeente. Deze zijn niet op één lijn te krijgen. Gevolg is dat de samen-werkende partners anders omgaan met de verwerking van (bijzondere) persoons-gegevens en allerlei onduidelijkheden ontstaan.

Een aantal afspraken die in de hoofd- en bewerkersovereenkomst met de leverancier moeten nog nader uitgewerkt worden. Het exitplan is nog niet opgesteld en de uitwijklocatie is nog niet operationeel. Bovendien beschikt de softwareleverancier nog niet over de vereiste ISO certificering ten behoeve van de beveiliging. De sturing op het nakomen van de afspraken met de leverancier is daarom nog niet optimaal.

De autorisaties in RIS zijn in sommige gevallen te ruim. In de praktijk blijkt dat bepaalde medewerkers toegang krijgen tot gegevens van cliënten die vanuit hun taakuitoefening niet noodzakelijk zijn. Toezicht hierop door middel van analyses op de logging vindt vooralsnog niet actief plaats.
Bij Samen DOEN is door de mogelijkheid om bepaalde cliëntgegevens te exporteren een reëel risico voor privacyschending aanwezig. Daarnaast zijn er nog risico's door gegevens die via een onbeveiligd kanaal verzonden worden.

Er is beperkt aandacht voor concernbrede opleidingen voor privacy(bewustzijn). Tot nu toe heeft dit enkel geleid tot plannen en voornemens op concernniveau. Het heeft nog niet geleid tot een daadwerkelijke uitvoering.
Binnen het cluster Sociaal vinden er wel deelopleidingen plaats, maar in de meeste gevallen zijn deze niet nadrukkelijk gericht op privacy. Als enige heeft OKT de eerste stappen gezet om privacy binnen de leerlijn op te nemen. Ook het aanstellen van de aandachtsfunctionaris voor privacy bij Samen DOEN is positief. Er is wel meer

structurele aandacht nodig voor het bespreken van en het leren over privacy. De lerende organisatie moet op dat vlak nog een concrete gestalte krijgen.
De belangrijkste vraagbaken voor de hulpverleners bij privacyvraagstukken blijkt de casuïstiekoverleggen te zijn. Deze overleggen zijn casusgericht, en privacy komt hierin incidenteel naar voren als gespreksonderwerp, op initiatief van de professional zelf.

Privacyschouw Jeugd is een goed instrument om privacy binnen OKT onder de aandacht te brengen. Bovendien heeft het geleid tot de implementatie van meerdere maatregelen. De schouw is echter wel eenmalig en is niet cyclisch van karakter. Halverwege januari 2016 heeft college van B en W aangegeven maatregelen te zullen treffen om de bewustwording over privacy bij medewerkers te zullen vergroten, de kaders voor het borgen van de taken en verantwoordelijkheden te zullen actualiseren, het toezicht op de naleving van privacywetgeving te versterken, de bewerkers-overeenkomsten te actualiseren en te zullen anticiperen op nieuwe wetgeving.

5 Hoe is het proces rondom de burger geregeld?

Naast de organisatorische afspraken die zijn gemaakt om privacywaarborgen te organiseren (hoofdstuk 3 en 4) zijn er ook afspraken gemaakt die primair gericht zijn om de directe interactie met de burger. In dit hoofdstuk wordt de vierde onderzoeksvraag beantwoord:

Hoe is het proces rondom de cliënt geregeld en sluit dit voldoende aan op de Wbp?

Het gaat daarbij om burgers of wettelijke vertegenwoordigers die een beroep doen op de ondersteuning of hulpverlening door Samen DOEN, OKT en Wijkzorger. In lijn met de Wet bescherming persoonsgegevens (Wbp) spreken we in dit hoofdstuk verder van *betrokkene* in plaats van burger of zijn of haar wettelijke vertegenwoordiger. De *betrokkene* is degene op wie een persoonsgegeven betrekking heeft.

Waar de focus in de vorige hoofdstukken ligt op de organisatiebrede afspraken en de afspraken binnen jeugd en zorg, ligt de focus in dit hoofdstuk op de afspraken die gemaakt zijn voor Samen DOEN, OKT en Wijkzorg.

Deze afspraken raken het gehele proces van gegevensverwerking en de daaraan ten grondslag liggende uitgangspunten. Het proces van *gegevensverwerking* omvat het gehele proces dat een gegeven doormaakt. Het start met het moment van verzamelen van gegevens waarna deze gegevens worden gebruikt en eventueel gedeeld. Het proces eindigt met het moment van vernietiging van gegevens. De uitgangspunten hebben onder meer betrekking op de grondslagen en doelen van gegevensverwerking, maar ook op geheimhouding en wie verantwoordelijk voor de gegevensverwerking is.

De afspraken zijn vooral vastgelegd in drie privacyprotocollen. Voor elke van de drie samenwerkingsketens – Samen DOEN, OKT en Wijkzorg – is er één protocol. De algemene uitgangspunten, de voorlichting aan de betrokkene en de diverse processtappen hebben wij getoetst aan de normen uit de Wet bescherming persoonsgegevens (Wbp), met als doel om een uitspraak te doen over de mate waarin de privacyprotocollen in lijn zijn met de Wbp om zo te kunnen bepalen of de privacy voor de betrokkene in opzet is geborgd. De normen uit de Wbp hebben wij per paragraaf samengevat weergegeven. Een uitgebreide toelichting op de normen is te vinden in bijlage 2.

5.1 Algemene uitgangspunten bij verwerken van persoonsgegevens

5.1.1 Grondslag(en)

Normen vanuit de Wbp
De Wbp kent uitputtende grondslagen voor het verwerken van persoonsgegevens.[326] Voor het sociaal domein geldt dat persoonsgegevens slechts mogen worden verwerkt op grond van een *wettelijke verplichting* of op grond van de *vervulling van een publiekrechtelijke* taak. Slechts bij uitzondering kan verwerking van persoonsgegevens bij de Wmo plaatsvinden als de betrokkene zijn *ondubbelzinnige toestemming* heeft verleend. In de andere gevallen zal er sprake zijn van een afhankelijkheidsrelatie tussen de betrokkene en de gemeente of hulpverlener waardoor er van ondubbelzinnige toestemming geen sprake kan zijn (zie voor een uitgebreide toelichting bijlage 2).

Elk privacyprotocol bevat een overzicht van grondslagen waarop de gegevensverwerking zou zijn gebaseerd. Afhankelijk van het privacyprotocol varieert het aantal opgegeven grondslagen tussen de 6 en 11. Slechts de Jeugdwet, Wet publieke gezondheid en de Wmo geven de wettelijke verplichting of publiekrechtelijke taak op grond waarvan kan worden beoordeeld of de verwerking een rechtmatige grondslag heeft (zie tabel 5.1).

Tabel 5.1 - Grondslagen gegevensverwerking Samen DOEN, OKT en Wijkzorg

Grondslagen	Samen DOEN [327]	OKT[328]	Wijkzorg[329]
Jeugdwet en besluit jeugdwet	x	x	
Wet publieke gezondheid		x	
Wet maatschappelijke ondersteuning	x	x	x

X= grondslag wordt expliciet genoemd in privacyprotocol

De overige wetten, beroeps- en gedragscodes, handreiking en privacyreglementen (zie tabel 5.2) geven randvoorwaarden voor een zorgvuldige verwerking van persoonsgegevens maar kunnen niet worden aangemerkt als een grondslag zoals bedoeld in art 8 van de Wbp.

[326] Zie art. 8 Wbp
[327] Privacyprotocol Samen DOEN, art. 18, lid 1
[328] Privacyprotocol Ouder- en Kindteams, art. 18, lid 1
[329] Privacyprotocol Wijkzorg, art. 17, lid 1

Tabel 5.2 - Randvoorwaarden zorgvuldige gegevensverwerking

Randvoorwaarden	Samen DOEN [330]	OKT[331]	Wijkzorg[332]
Wet bescherming persoonsgegevens	x	x	x
Wet inzake de geneeskundige behandelingsovereenkomst	x	x	x
Leerplichtwet	x	x	
Beroepscode van de Nederlandse Vereniging van Maatschappelijk Werkers	x	x	x
Beroepscode voor de Jeugdzorgwerker	x	x	
Gedragscode van het Nederlands Instituut voor Psychologen;	x	x	
Gedragscode van de Nederlandse Vereniging van Onderwijskundigen en Pedagogen	x	x	
Handreiking Bemoeizorg van KNMG, GGD Nederland en GGZ Nederland	x	x	x
Privacyreglementen van alle convenantpartners	x	x	
Privacyreglementen van de ketenpartners			x

In lijn met de Wmo wordt in het privacyprotocol Wijkzorg ook de uitdrukkelijke *toestemming van betrokkene* aangevoerd als grondslag. Aanvullend worden in het privacyprotocol Wijkzorg ook nog twee andere grondslagen genoemd voor de gegevensverwerking:

- het uitvoeren van een overeenkomst, waaronder in elk geval de overeenkomst die aanbieders van maatschappelijke ondersteuning met cliënten hebben.
- een goede vervulling van een publiekrechtelijke taak.

Conclusies

Elke gegevensverwerking is gebaseerd op één of meerdere grondslagen zoals bedoeld in de Wbp. De privacyprotocollen bevatten een te omvangrijke verwijzing naar allerlei regelgeving, beroeps- en gedragscodes en privacyreglementen om te motiveren wat de grondslagen zijn voor het verwerken van de gegevens. Een groot deel betreft meer randvoorwaarden voor een zorgvuldige gegevensverwerking.

5.1.2 Doel(en)

Normen vanuit de Wbp

Gegevensverwerking is alleen toegestaan als er sprake is van een uitdrukkelijk, gerechtvaardigd en welbepaald doel waarvoor de gegevens worden verzameld. Deze doelomschrijving moet duidelijk zijn, niet zo vaag of ruim bijvoorbeeld dat zij tijdens

[330] Privacyprotocol Samen DOEN, art. 18, lid 1

[331] Privacyprotocol Ouder- en Kindteams, art. 18, lid 1

[332] Privacyprotocol Wijkzorg, art. 17, lid 1

het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. Het verzamelen van gegevens over willekeurige burgers voor een doel dat mogelijk in de toekomst relevant zal zijn, is in beginsel niet toegestaan. De gegevensverwerking voldoet aan de beginselen van proportionaliteit en subsidiariteit.

De doelen van de verwerking van persoonsgegevens zijn opgenomen in de drie privacyprotocollen. Deze zijn voor Samen DOEN, OKT en Wijkzorg in de onderstaande tabel beschreven.

Tabel 5.3 - Doelen per samenwerkingsketen

Samen DOEN[333]	**Ouder- en Kindteams**[334]	**Wijkzorg**[335]
Uitvoering van de wettelijke taken en werkzaamheden zoals vermeld in de Jeugdwet en de Wet maatschappelijke ontwikkeling door de wijkteams Samen DOEN.	Uitvoering van de wettelijke taken en werkzaamheden zoals vermeld in de Jeugdwet en de Wet publieke gezondheid door OKT.	Het op basis van de Wmo 2015 op effectieve wijze hulp en ondersteuning te verlenen in het kader van Wijkzorg. Het einddoel van iedere ondersteuning is het bevorderen van de zelfredzaamheid en participatie, voorkomen van achteruitgang of begeleiden bij achteruitgang van een persoon.
Genereren van niet op betrokkenen herleidbare informatie in de vorm van statistische en andere overzichten voor beheer-, beleids- en onderzoeksdoeleinden	Genereren van niet tot de persoon herleidbare informatie in de vorm van statistische en andere overzichten voor beheer-, beleids- en onderzoeksdoeleinden	Niet op betrokkenen herleidbare gegevens genereren in de vorm van statistische en andere overzichten voor beheer-, beleids- en onderzoeksdoeleinden

In alle drie de protocollen is aangegeven dat een adviseur alleen persoonsgegevens verwerkt voor zover dat voor een goede hulpverlening aan betrokkene noodzakelijk is.[336]

[333] Privacyprotocol Samen DOEN, art. 3, lid a-b.

[334] Privacyprotocol Ouder- en Kindteams, art. 3, lid a-b.

[335] Privacyprotocol Wijkzorg, art. 3, lid 1-2.

[336] Privacyprotocol Samen DOEN, art. 18, lid. 2-4, Privacyprotocol Ouder- en Kindteams, art. 18, lid 2-4 en Privacyprotocol Wijkzorg, art. 17, lid 2-3.

Conclusies
De doelen waarvoor de gegevens worden verzameld zijn welbepaald en gerechtvaardigd. De doelen zijn echter niet voorafgaande aan de gegevensverzameling aan papier toevertrouwd, maar pas opgesteld nadat de gegevensverzamelingen er al waren. De doelomschrijvingen zijn duidelijk, namelijk het kunnen uitvoeren van de wettelijke taken en het generen van o.a. beleids-informatie. De doelen zijn echter zo ruim gesteld dat het niet goed mogelijk is om in een individueel geval vast te stellen dat de gegevens voor het juiste doel zijn verwerkt. Hierdoor kan niet worden vastgesteld dat altijd overeenkomstig de Wbp wordt gehandeld wanneer het protocol wordt gevolgd.

Positief is dat de beperking is opgelegd dat gegevens alleen worden verwerkt voor zo ver dat voor een goede hulpverlening aan betrokkene noodzakelijk is. Een expliciete afweging van het proportionaliteits- en subsidiariteitsbeginsel zien wij beperkt terug in de privacyprotocollen. Bij OKT wordt in de privacyworkshops wel aandacht besteed aan (de afweging van) proportionaliteit en subsidiariteit door professionals een afwegingskader te bieden voor situaties waarin ze overwegen of ze gegevens moeten delen. Dit afwegingskader is een set vragen die samen de uitwerking zijn van de begrippen proportionaliteit en subsidiariteit en. Deze zijn ontleent aan het rapport 'Samenwerken in de Jeugdketen, een instrument voor gegevensuitwisseling' van het ministerie van VWS.

5.1.3 Geheimhouding

Normen vanuit de Wbp
Gegevens worden geheimgehouden, tenzij hier een inbreuk op moet worden gemaakt vanuit een wettelijke plicht of vanuit de taak.

Iedereen die kennis neemt van persoonsgegevens die zijn verwerkt zoals bedoeld in het protocol van Samen DOEN, OKT en Wijkzorg, is verplicht tot geheimhouding daarvan, tenzij de wet of de werkwijze zoals uiteengezet in het protocol anders bepaalt.[337]

Conclusie
De drie privacyprotocollen zijn op het punt van geheimhouding in lijn met de Wbp.

5.1.4 Verantwoordelijke en passende beveiliging

Normen vanuit de Wbp - verantwoordelijke
De strekking van art 14 lid 1 is om te voorkomen dat bij eventuele tekortkomingen in de gegevensverwerking, verantwoordelijke en bewerker zich wat betreft hun verantwoordelijkheden achter elkaar zouden kunnen verschuilen. De verplichtingen moeten over en weer duidelijk zijn neergelegd. Op de verantwoordelijke rust een zorgplicht daarvoor zorg te dragen.

[337] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 20; privacyprotocol Wijkzorg, art. 18.

Niet alleen dient hij civielrechtelijk de bewerker voldoende te hebben duidelijk gemaakt hoe met de persoonsgegevens wordt omgegaan, tevens dient hij toe te zien op de feitelijke naleving van de aldus gecreëerde verplichtingen.[338]
Normen vanuit de Wbp – passende beveiliging
De verantwoordelijke legt passende technische en organisatorische maatregelen ten uitvoer om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. De maatregelen zijn er mede op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen.[339]

Per samenwerkingsverband - Samen DOEN, OKT en Wijkzorg - is gekozen voor één gezamenlijke verantwoordelijke (zie ook paragraaf 3.3.1).[340]

Het college stuurt de leverancier (bewerker) aan zodat deze voldoet aan de organisatorische en technische wettelijk geldende vereisten met betrekking tot de informatiebeveiliging passend bij het niveau waarop (bijzondere) persoonsgegevens worden verwerkt.[341] De gegevens moeten daarbij beveiligd zijn tegen verlies, enige vorm van onrechtmatige verwerking, ongeautoriseerde kennisneming en onnodige verzameling en verdere verwerking van gegevens.[342]

De instellingen die de samenwerkingsovereenkomst hebben getekend en daarmee participeren in Samen DOEN, OKT en Wijkzorg zijn verantwoordelijk voor de verwerking van de persoonsgegevens in het kader van de door adviseurs te leveren hulp en het treffen van nodige maatregelen zodat de te verwerken persoonsgegevens juist en niet bovenmatig zijn, gelet op de doeleinden waarvoor zij verzameld en verwerkt worden.[343] De partijen van Samen DOEN en OKT zijn gezamenlijk verantwoordelijk in de zin dat zij zorg dragen voor technische en organisatorische maatregelen zodat de wijkteams Samen DOEN op juiste wijze met persoonsgegevens omgaan. Tevens zijn de partijen met de vermelde taken in het protocol ten opzichte van elkaar aansprakelijk voor zorgvuldige en juiste verwerking van persoonsgegevens.[344] De verantwoordelijkheid voor de verwerking van de persoonsgegevens

[338] *Kamerstukken II*, 1997-1998, 25 892, nr 3, blz. 99.
[339] Art. 13 Wbp.
[340] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 17 lid 3; privacyprotocol Wijkzorg, art. 16 lid 1.
[341] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 17 lid 1; privacyprotocol Wijkzorg, art. 16 lid 3.
[342] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 21 lid 1; Privacyprotocol Wijkzorg, art. 20 lid1.
[343] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 17 lid 2; privacyprotocol Wijkzorg, art. 16 lid 2 en 5. In het privacyprotocol van Wijkzorg wordt dit aangevuld met: "*Dit betekent een zorgvuldige verwerking van persoonsgegevens van betrokkenen, de borging van juistheid, noodzaak en kwaliteit van de gegevens.*"
[344] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 21 lid 2.

van de cliënt in het kader van Wijkzorg is belegd bij de gezamenlijke partijen die Wijkzorg uitvoeren.[345] Afgesproken is dat alle partijen bij Wijkzorg afzonderlijk verantwoordelijk zijn voor de programmatuur en informatiebeveiliging van hun eigen systemen. Bij Wijkzorg mag behalve het systeem RIS ook gebruik worden gemaakt van systemen van de moederorganisatie.[346] De partijen dragen tevens zorg dat de bewerker de verplichtingen naleeft die op verantwoordelijke rusten ten aanzien van de beveiliging en zien toe op de naleving van die afspraken door de bewerker[347]. Voor de betrokken partijen gelden algemeen geaccepteerde autorisatie- en beveiligingsstandaarden en –normen die dienen als uitgangspunt voor het vaststellen van de risico's van de gegevensverwerking en passende maatregelen voor beveiliging.[348]

De instellingen dienen zorg te dragen voor de naleving van het privacyprotocol en voor de naleving van alle wettelijke verplichtingen met betrekking tot de bescherming van de persoonlijke levenssfeer van betrokkene.[349]

Zoals in paragraaf 3.3.1 is aangeven is het voor betrokkene van belang om te weten welke entiteit de verantwoordelijke is als een gang naar de rechter moet worden gemaakt. Het protocol geeft de betrokkene hierover geen uitsluitsel.

5.1.5 Conclusies

Afgesproken is dat de afzonderlijke samenwerkingsverbanden - Samen DOEN, OKT, Wijkzorg – de verantwoordelijken zijn in de zin van de Wbp. Het samenwerking-sverband is daarmee verantwoordelijk dat de gegevensverwerking aan de eisen van de Wbp voldoet. Hiertoe zijn afspraken gemaakt tussen de samenwerkende partijen, waaronder de afspraak dat het niveau van informatiebeveiliging bij de ketenpartners passend is. Het samenwerkingsverband is ook verantwoordelijk voor het toezicht op de naleving van de gemaakte afspraken. Dit toezicht is onvoldoende geregeld (zie ook paragrafen 3.6 en 4.5) waardoor het signaleren van afwijkingen van de Wbp zeer moeilijk kan worden geconstateerd en optreden in de handhavende sfeer bijna onmogelijk is.[350] De mogelijkheid om te instrueren of sancties op te leggen, maakt geen onderdeel uit van de afspraken.

Onduidelijk is bovendien of een betrokkene de bestuursrechtelijke of civielrechtelijke rechtsgang moet volgen als hij de verantwoordelijke voor de rechter wil dagen. De rechtsbescherming voor de betrokkene zou op dit punt kunnen worden verbeterd.

---

[345] Privacyprotocol Wijkzorg, art. 16 lid 1 met inachtneming van het bepaalde art. 5.1.1 en 5.1.2 van de Wmo 2015

[346] Privacyprotocol Wijkzorg, art. 16 lid 2.

[347] Privacyprotocol Wijkzorg, art. 20 lid 2.

[348] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 21 lid 3; Privacyprotocol Wijkzorg, art. 20 lid 3.

[349] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 17 lid. 3; privacyprotocol Wijkzorg, art. 16 lid 4.

[350] Een gedeeltelijke uitzondering hierop vormt Wijkzorg waarbij in art 17 van de raamovereenkomst is bepaald dat een boetebeding van kracht is wanneer de veiligheid van een cliënt in het geding is gekomen.

5.2 Is de kennis van privacyregelgeving van ambtenaren en hulpverleners voldoende?

Normen vanuit de Wbp
Persoonsgegevens worden in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt.[351]

In de samenwerkingsovereenkomst Samen DOEN en OKT is opgenomen dat door plaatsing van teamleden vanuit verschillende disciplines de Samen DOEN buurtteams uit teamleden bestaan met zoveel mogelijk verschillende relevante achtergronden en deskundigheid/ervaring. Hierdoor beschikt elk team van Samen DOEN en OKT over een zo groot mogelijk basisarsenaal aan gemeenschappelijke kennis en vaardigheden aangevuld met specifieke kennis en vaardigheden.[352] De teamleden van Samen DOEN werken volgens de Uniforme Werkwijze en met achtneming van het opgestelde privacyprotocol. De knelpunten over de uitvoering en aansturing worden zo veel mogelijk binnen het Samen DOEN buurtteam opgelost.[353] Ouder- en Kindteams hebben de taak te zorgen voor de uitvoering van het vastgestelde werkplan met betrekking tot geboden OKT zorg.[354]

Conclusie
De rekenkamer vindt kennis van de Wbp een randvoorwaarde voor een goede taakuitoefening door ambtenaren en hulpverleners. Kennis van de Wbp is een voorwaarde om overeenkomstig de Wbp te kunnen handelen. In de samenwerkingsovereenkomsten Samen DOEN en OKT is dit uitgangspunt impliciet geregeld door te stellen dat bij het handelen het privacyprotocol in acht moet worden genomen. Voor Wijkzorg is op dit punt niets geregeld.

5.3 Voorlichting

Normen vanuit de Wbp
Een betrokkene moet in beginsel altijd op de hoogte zijn van het feit dat zijn gegevens worden verwerkt, door wie zijn gegevens worden verwerkt en voor welke doeleinden zijn gegevens worden verwerkt.

Uitgangspunten VNG
In de *Handreiking communiceren met burgers over privacy* van de VNG worden gemeenten geadviseerd over hoe de burger actief te informeren over het verwerken van persoonsgegevens. Op deze manier kan de burger erop vertrouwen dat er zorgvuldig met zijn gegevens wordt omgegaan en de gegevens bij de gemeente en instanties veilig zijn.

[351] Art. 6 Wbp.
[352] Samenwerkingsovereenkomst Samen DOEN, oktober 2014, art. 5 lid 5.
[353] Samenwerkingsovereenkomst Samen DOEN, oktober 2014, art. 5 lid 6.
[354] Samenwerkingsovereenkomst Ouder- en Kindteams, oktober 2014, art. 5 lid 6.

De handreiking geeft een drietal punten aan die in elk geval van belang zijn bij het actief voorlichten van burgers.

1. Communiceer via meerdere kanalen.
   - *Mondeling tijdens contactmomenten*. Tijdens de contactmomenten (bijvoorbeeld tijdens een keukentafelgesprek of bij het KlantContactCentrum) moet de burger actief worden geïnformeerd wat er met zijn/haar gegevens gebeurt.
   - *Website.* Informeer de burger via de website van de gemeente over de verwerking van persoonsgegevens. Zorg dat deze tekst helder is geformuleerd en voor de burger gemakkelijk vindbaar is.
   - *Folder.* Stel een folder op over de verwerking van persoonsgegevens en neem hierin ook op welke rechten de burger heeft met betrekking tot het verwerken van persoonsgegevens. Het wordt aangeraden de folder tijdens contactmomenten aan de burger te geven.
2. Wees transparant tijdens de triagemomenten (alle momenten waarop een afweging wordt gemaakt over het verhelderen, routeren of escaleren van vragen en casussen; zie ook paragraaf 5.4.4.)
3. Wijs de burger actief op zijn/haar rechten. Wijs de burger altijd op het recht om een formeel verzoek in te dienen ter inzage, wijziging of verwijdering van zijn/ haar persoonsgegevens. Zorg dat het voor de burger duidelijk is tot welke instantie zij zich moeten wenden.[355]

Algemene uitgangspunten voorlichting

De Wethouder Jeugd ziet een actieve rol voor de gemeente in het voorlichten van burgers over hun rechten en plichten bij privacy. Naast voorlichting via de website van de gemeente en specifiek op de website van OKT[356], maken adviseurs tijdens het eerste gesprek duidelijk hoe wordt omgegaan met persoonsgegevens en welke rechten de leden van het huishouden hebben.[357] Tevens reiken de drie samenwerkingsverbanden - Samen DOEN, OKT en Wijkzorg - voorlichtingsmateriaal uit. Binnen de privacyschouw (zie ook paragrafen 3.5.3 en 4.4.2) zal het verschillende voorlichtingsmateriaal worden vergeleken om te bepalen of er behoefte is aan meer uniforme voorlichting, of dat het gescheiden moet blijven.[358]

Voorlichting vindt ook plaats via de preambule in het privacyprotocol. Daarin is beschreven wat de betrokkene aan ondersteuning kan verwachten, dat daarbij persoonsgegevens worden verwerkt en dat de betrokkene daarover moet worden ingelicht. Dit geldt ook voor de rechten en plichten die de betrokkene heeft.[359] Het onderdeel triagemomenten bij de voorlichting wordt behandeld in paragraaf 5.4.4. In paragraaf 6.3 wordt ingegaan op de vindbaarheid van informatie, onder meer op de website.

[355] VNG, Handreiking communiceren met burgers over privacy, december 2014, p. 1.

[356] Zie www.oktamsterdam.nl onderdeel Veel gestelde vragen: *Hoe gaat het Ouder- en Kindteam om met mijn privacy?*.

[357] Preambule van Privacyprotocol Ouder- en Kindteams, Samen DOEN, Wijkzorg preambule.

[358] Interview, 08-12-2015.

[359] Gespreksverslag, 10-11-2015 hierin werd gesteld dat de preambule is geschreven voor de burger.

Conclusie
De voorlichting is in lijn met de Wbp en grotendeels, uitgezonderd de triagemomenten, met de normen van de VNG.

5.4 Registratie van persoonsgegevens

Normen vanuit de Wbp
De verantwoordelijke heeft de plicht om de betrokkene tijdig te informeren over gegevensverwerking.
Maatregelen zijn getroffen opdat de persoonsgegevens juist, nauwkeurig, toereikend, ter zake dienend en niet bovenmatig zijn, gelet op de doel(eind)en.
Overheidsorganisaties, zorgaanbieders (dus ook jeugdzorggeneralisten) mogen het burgerservicenummer (BSN) gebruiken om hun taak uit te voeren, maar alleen als het BSN hierbij noodzakelijk is. Organisaties buiten de overheid mogen het BSN alleen gebruiken als dit in een specifieke wet is bepaald en alleen voor het specifieke doel dat in de wet staat omschreven.

5.4.1 Informeren betrokkene

In de preambule van de privacyprotocollen van Samen DOEN, OKT en Wijkzorg staat beschreven dat de klanthouder in gesprek gaat met de betrokkene en voorafgaand aan of in het eerste gesprek uitlegt hoe wordt omgaan met (bijzondere) persoonsgegevens en welke rechten de betrokkene heeft.[360] De adviseur heeft een registratieplicht en informeert het huishouden hierover.

In het privacyprotocol *Samen DOEN* staat beschreven welke informatie de buurtteammedewerker aan de betrokkene dient te verstrekken. In het eerste gesprek dient te worden aangegeven hoe wordt omgegaan met persoonsgegevens, welke rechten de betrokkene heeft, dat de adviseur een geheimhoudingsplicht en dossier- en registratieplicht heeft, en in welke gevallen gegevens verwerkt en gedeeld worden en hoe dat gebeurt.[361] In het protocol staat dat het protocol door iedereen op de internetsite van de gemeente Amsterdam en op de site van de wijkteams Samen DOEN kan worden geraadpleegd.[362]

Ook in het privacyprotocol *OKT* wordt gemeld dat de adviseur de betrokkenen altijd de werkwijze van de OKT teams uitlegt en vermeldt in welke gevallen gegevens verwerkt, geregistreerd of gedeeld worden en op welke wijze.[363]

[360] Privacyprotocol Samen DOEN, preambule.
[361] Privacyprotocol Samen DOEN versie 2, okt 2015.
[362] Privacyprotocol Samen DOEN versie 2, oktober 2015, art. 23 lid. 3.
[363]Privacyprotocol OKT, art 5 'Informeren over gegevensverwerking'.

Uit het privacyprotocol *Wijkzorg* blijkt dat de klanthouder de betrokkene tijdens het eerste klantcontact moet wijzen op de manier waarop er wordt omgegaan met zijn/haar gegevens en welke rechten de betrokkene heeft.[364] De rechten betreffen rechten die voortkomen uit de Wbp en rechten binnen de klachtenprocedure.[365] De klanthouder dient gedurende de tijd dat hij de betrokkene ondersteunt steeds uit te leggen wat hij doet, wanneer hij gegevens registreert en wanneer hij gegevens beschikbaar stelt aan deskundigen die betrokken zijn bij de hulpvraag[366]. In de *factsheet Klachten WMO* staat bovendien dat de professional de betrokkene adviseert over de klachtenregeling van de Gemeente Amsterdam.

Voor Wijkzorg geldt dat staat aangegeven welke informatie direct bij het eerste contact mondeling en schriftelijk dient te worden verstrekt. Dit betreft de volgende informatie:

- dat gegevens over de cliënt worden verwerkt, opgeslagen en indien nodig verstrekt
- de identiteit van de klanthouder
- informatie over procedures rondom Wijkzorg
- informatie over de mogelijkheid van een second opinion, de mogelijkheid van de onafhankelijke cliëntondersteuner en de mogelijkheid van het aanleveren van een persoonlijk plan
- de rechten en plichten van de cliënt, waaronder ook de rechten vanuit de Wbp en de klachtenprocedure
- informatie over de eigen bijdrage en het persoonsgebonden budget. [367]

In het privacyprotocol van Samen DOEN en OKT staat dat voordat de adviseur enige ondersteuning of hulp biedt, hij de betrokkene de werkwijze van het wijkteam toelicht en vermeldt in welke gevallen hij gegevens verwerkt (registreert en deelt) en op welke wijze.[368]

5.4.2 Toestemming betrokkene

In de drie protocollen wordt gesteld dat ondersteuning of hulpverlening (van Samen DOEN, OKT en Wijkzorg) op vrijwillige basis is. Degene die de ondersteuning, hulp of zorg ontvangt of diens verzorgers of diens bevoegde vertegenwoordigers gaan volgens het protocol akkoord met de geboden ondersteuning en hulpverlening door deze te accepteren. [369] Hulp en ondersteuning brengen met zich mee dat (bijzondere) persoonsgegevens ook worden geregistreerd.[370] Toestemming is volgens de protocollen voor het registreren dus in de regel niet aan de orde tenzij:

---

[364] Privacy protocol Wijkzorg p. 2.

[365] Privacy Protocol, Artikel 6: het registeren van gegevens.

[366] Privacy protocol, pagina 2.

[367] Privacyprotocol Wijkzorg, Artikel 6, lid 2.

[368] Privacyprotocol Samen DOEN en OKT, artikel 5.

[369] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 1; Privacyprotocol Wijkzorg, art. 8 lid. 1.

[370] Zie preambule van het privacyprotocol Samen DOEN en Ouder- en Kindteams en het Interview van 26 oktober 2015.

- het opvoed- en opgroeiondersteuning betreft. In dat geval vraagt de adviseur de betrokkene vooraf toestemming voor de gegevensverwerking van (bijzondere) persoonsgegevens.[371] Bij groepstraining wordt toestemming gevraagd om de contactgegevens te mogen registreren.[372] of,
- het betreft jeugdhulp (WGBO) of ondersteuning op grond van de Wet Publieke gezondheid door OKT. Ook in dat geval wordt de betrokkene geacht vooraf in te stemmen. De adviseur informeert de betrokkene vervolgens over de dossierplicht, zijn verplichting te registreren en zijn geheimhoudingsplicht.[373]

Bovenstaande is een wijziging die vanaf oktober 2015 doorgevoerd in de protocollen. Voor die tijd was het in alle situaties verplicht expliciet toestemming te vragen voor de registratie van persoonsgegevens.

In lijn met de Wmo is in de preambule van het privacyprotocol Wijkzorg wel vermeld dat gegevens alleen worden geregistreerd met toestemming van de betrokkene. Dit toestemmingsrecht ontbreekt echter in de bepalingen van het protocol.[374]

5.4.3 Automatische of impliciete toestemming betrokkene

De privacyprotocollen bevatten de bepalingen dat degene die de ondersteuning, hulp of zorg ontvangt of diens verzorgers impliciet akkoord zijn met de geboden ondersteuning en hulpverlening door deze te accepteren.[375] Daar waar bij Samen DOEN voor opvoed- en opgroeiondersteuning en jeugdhulp expliciete toestemming van de betrokkene nodig is, wordt toestemming voor de andere hulpverlening verondersteld. Zo ook in het geval van collegiale toetsing of samenwerking bij een specifieke hulpvraag. [376]

5.4.4 Vast te leggen gegevens

In de protocollen is geregeld welke (bijzondere) persoonsgegevens verwerkt worden (zie tabel 5.4).

[371] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 2.

[372] Privacyprotocol Samen DOEN en Ouder- en Kindteams, preambule.

[373] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 3.

[374] Zie art 5.1.1. Wmo en Privacyprotocol Wijkzorg preambule.

[375] Privacyprotocol Samen DOEN en Ouder- en Kindteams art 9 lid ; Wijkzorg art 8 lid 1.

[376] Privacyprotocol Samen DOEN art 9 lid 4. Wel informeert de adviseur de betrokkene hierover en over de mate waarin de persoonsgegevens gedeeld worden.

Tabel 5.4 -Te verwerken (bijzondere) persoonsgegevens

Verwerkte (bijzondere) persoonsgegevens	Samen DOEN[377]	OKT[378]	Wijkzorg[379]
Naam, adres en BSN van betrokkene	x	x	x
Geslacht, geboortedatum, telefoonnummer			x[380]
Huisarts			x
Familie- en sociale relaties	x	x	
Gegevens over verblijfsstatus	x	x	
Woon-, werk-, schoolsituatie	x	x	
Gegevens over de gezondheid	x	x	
Werkafspraken ter uitvoering van de taken van de wijkteams	x	x	x[381]
Onderzoeksgegevens die nodig zijn voor de uitvoering van de taken van wijkteams	x	x	
Financiële en administratieve gegevens	x		x[382]
Samenvatting uitkomsten conclusie van externe deskundigen	x	x	

Ook van bloedverwanten, aanverwanten of anderen die tot de sociale omgeving van de betrokkene horen kunnen gegevens worden verwerkt. De Jeugdwet en de Wmo bieden hiervoor een wettelijke grondslag. Worden gegevens over deze personen verwerkt dan moeten zij ook worden aangemerkt als betrokkene in de zin van de Wbp, met als gevolg dat ze ook alle bijbehorende rechten hebben, waaronder recht op voorlichting over de gegevensverwerking en het recht op inzage en correctie van gegevens.

De protocollen geven ook de mogelijkheid dat het burgerservicenummer (BSN) van andere betrokkenen, zoals bloedverwanten, aanverwanten of anderen die tot de sociale omgeving van de betrokkene horen wordt geregistreerd.

Uit werkinstructies blijkt dat in sommige gevallen bepaalde gegevens wel worden opgeslagen, terwijl deze niet in het privacyprotocol worden benoemd. Dit geldt voor het telefoonnummer en geboortedatum bij Samen DOEN.[383] De gegevenssets in het privacyprotocol lijken daardoor niet altijd volledig.

Voor Samen DOEN en Wijkzorg geldt dat de adviseur ook gegevens verzamelt met behulp van de zelfredzaamheidsmatrix (ZRM) over de mate van zelfredzaamheid van

[377] Privacyprotocol Samen DOEN, art. 6 lid 2.

[378] Privacyprotocol Ouder- en Kindteams, art. 6 lid 2.

[379] Bijlage IV RIS gegevensset, 23 februari 2015.

[380] Bij Wijkzorg is dit in een aparte bijlage van het privacyprotocol opgenomen.

[381] Het betreft hier het ondersteuningsplan.

[382] Voor zover het inkomsten betreft.

[383] Handleiding Registratieproces in RIS, versie 2, April 2015

het huishouden (zie kader).[384] Bij Samen DOEN wordt de ZRM ingezet om de voortgang op zelfredzaamheid van de cliënt te kunnen monitoren. Tevens wordt de ZRM ingevuld om de effectiviteit van het programma Samen DOEN te kunnen monitoren en evalueren. Het niet invullen van de ZRM heeft dus directe gevolgen voor deze monitor.[385] Bij Wijkzorg gebruiken professionals de Zelfredzaamheid-Matrix als een meetinstrument om het functioneren van cliënten en van de zorg beter in kaart te kunnen brengen. De ZRM kan bij RIS-Wijkzorg voor kortdurende zorg niet langer worden ingevuld.

Een positieve uitzondering vormt daarop de dienstverlening aan burgers bij de Ouder- en Kindcentra op het moment dat zij komen voor informatie, advies, een themabijeenkomst of een preventieve training. Van hen wordt geen dossier in RIS aangemaakt.[386] Wel worden contactgegevens (telefoonnummer en eventueel adres) opgeslagen om bijvoorbeeld informatie rondom de training te kunnen communiceren. Dit laatste gebeurt uitsluitend met toestemming van de cliënt en gegevens worden alleen gebruikt voor het doel waarvoor de gegevens verzameld zijn.[387]

Zelfredzaamheidsmatrix

Met behulp van de zelfredzaamheidsmatrix wordt de zelfredzaamheid van personen en gezinnen ingeschat, met als doel te bepalen welke hulp vanuit de sociale omgeving van de persoon kan worden gemobiliseerd, wat de persoon zelf kan en welke hulp de gemeente moet bieden. In het kader van de zelfredzaamheidsmatrix wordt op 13 domeinen de zelfredzaamheid in kaart gebracht.
De volgende domeinen worden onderscheiden:

- Inkomen
- Huisvesting
- Geestelijke gezondheid
- Verslaving
- Sociaal netwerk
- Justitie[388]
- Dagbesteding
- Gezinsrelaties
- Fysieke gezondheid
- ADL – vaardigheden
- Maatschappelijke participatie
- Ouderschap

[384] Privacyprotocol Samen DOEN, art. 6 lid 3 en 4 Privacyprotocol Ouder- en Kindteams, art. 6 lid 3.
[385] Stedelijk directeur sociaal, feitelijk wederhoor, 17-02-2016
[386] Handleiding RIS-OKT, Gemeente Amsterdam, Januari 2015
[387] Bron: Mail, 8 februari 2016. De contactgegevens worden in een onderdeel van RIS vastgelegd waar alleen de trainer bevoegd is. Ook wordt geregistreerd hoeveel mensen (in aantallen) hebben deelgenomen aan een training. Op het moment dat een adviesvraag uitloopt in een vraag die meerdere gesprekken vereist, wordt voor de cliënt op dat moment een dossier aangemaakt in RIS.
[388] Toelichting op het veld ' justitie' afkomstig uit de ZRM: Zelfredzaamheid met betrekking tot justitie gaat over of de persoon op dit moment, of in het (recente) verleden, in aanraking is gekomen met politie en justitie. Wanneer de persoon op dit moment zaken bij justitie heeft lopen zou dat mogelijk kunnen interfereren met een eventueel zorg-, huisvesting- of dagbestedingtraject. Het hebben van een strafblad zou mogelijk invloed kunnen hebben op de arbeidstoeleiding. In veel gevallen zullen eerst justitiële zaken moeten worden gesloten voordat andere trajecten kunnen worden gestart. Politiecontacten gaan over alle staande- en aanhoudingen door politie voor een overtreding of misdrijf. Justitiële zaken zijn over het algemeen zaken met betrekking tot het strafrecht: 1= Cliënt krijgt straf. De cliënt moet voor de rechter verschijnen. Met name de huidige onzekerheid over de nabije toekomst maakt het een acuut probleem; 2 = Cliënt heeft straf. De cliënt zit in detentie, heeft een taakstraf, extramurale detentie (elektronisch toezicht), maar ook zgn. OM-transacties (voor bijvoorbeeld rijden zonder rijbewijs, of opgeven valse

- Tijdsbesteding

De beoordelaar vult op elk van de domeinen een score in. Deze score varieert van 'acute problematiek' (score 1) tot en met 'volledig zelfredzaam' (score 5). De andere scores zitten daar tussen in.
De zelfredzaamheidmatrix wordt op persoonsniveau vastgelegd (18 jaar en ouder). Indien er binnen een huishouden meerdere personen aanwezig zijn dan wordt voor elke persoon een zelfredzaamheidsmatrix ingevuld, tenzij beargumenteerd is aangegeven dat dit niet hoeft.

In de Privacy Impact Assessment (PIA) van het Rijk (november 2014) wordt aanbevolen om terughoudend te zijn met het vastleggen van persoonsgegevens en de principes van 'dataminimalisatie' en need-to-know in plaats van nice to know toe te passen en de afweging te maken wanneer kan worden volstaan met 'dat'-informatie en wanneer zogeheten 'wat'-informatie noodzakelijk is.[389] Juist bij de drie soorten afwegingsmomenten (eerste contact met de burger waarin de hulpvraag verhelderd moet worden, bij de behoeftebepaling en planvorming en tot slot bij escalatie) wordt een bewuste afweging van belang geacht, waarbij wordt bepaald welke gegevens noodzakelijk zijn om vast te leggen.[390] Gepleit wordt om deze afwegingen vast te leggen zodat deze transparant, expliciet en verifieerbaar zijn. [391]

De bewuste afwegingsmomenten die de professional maakt worden ook wel *triage* genoemd. Door middel van triage bepaalt een ambtenaar of professional of er sprake is van een enkelvoudige of meervoudige vraag, dan wel complexe (multiprobleem) casuïstiek en welke mate van gegevensverwerking daarbij hoort. Bij een eenvoudige, enkelvoudige vraag is de gegevensverwerking beperkter, terwijl bij een complexere vraag wellicht meer partijen betrokken zijn en meer gegevens verwerkt en gedeeld worden.[392] In de werkwijzers en protocollen wordt niet beschreven dat persoonsgegevens moeten worden beoordeeld en eventueel aangepast na een triage moment.

In de instructies voor de gebruikers van de ZRM is terughoudendheid niet het uitgangspunt. Gebruikers wordt aanbevolen om alle domeinen van de ZRM te scoren en te motiveren waarom persoonsgegevens voor een bepaald domein niet zijn uitgevraagd.[393]

5.4.5 Conclusies

De drie privacyprotocollen zijn op het punt van het informeren van de betrokkene op hoofdlijnen in lijn met de Wbp. Informeren van de betrokkene is de regel. Expliciete

---

identiteitsgegevens) e.d. ; 3= Cliënt heeft geen straf (meer) mits hij zich aan door de rechter gestelde voorwaarden houdt; 4 = Cliënt heeft straf gehad.

[389]Minister van Binnenlandse Zaken en Koninkrijksrelaties, Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Aandachtspunten, risico's en suggesties voor gegevensverwerking bij de uitvoering van de gemeentelijke taken en werkzaamheden in een gedecentraliseerd sociaal domein, 7 november 2014, p. 23

[390] Zie voetnoot 389, p. 22 en 23.

[391]Zie voetnoot 389, p. 23.

[392] Rapport Privacy Impact Assessment Gemeentelijke 3D Informatiehuishouding, Rijksoverheid, nov 2014, p. 22.

[393] Zie bijvoorbeeld Gebruikshandleiding RIS wijkzorg, 19 januari 2015, p. 16.

toestemming wordt alleen gevraagd bij opvoed- en opgroeiondersteuning, bij jeugdhulp (Jeugdwet) of ondersteuning op grond van de Wet publieke gezondheid door de Ouder- en Kindteams. In het privacyprotocol Wijkzorg is onvoldoende geregeld dat gegevens alleen worden geregistreerd met toestemming van de betrokkene.

De privacyprotocollen bevatten een bepaling voor automatische of impliciete toestemming. Dit vinden wij niet zorgvuldig. De toestemming is immers niet geverifieerd bij de betrokkene en de betrokkene kan worden tegengeworpen dat hij zelf met de gegevensverwerking en de verdere gevolgen daarvan akkoord is gegaan. Bovendien zullen niet-juridisch geschoolden (betrokkene, maar ook ambtenaren en professionals) zich er niet van bewust zijn dat de automatische toestemming niet betekent dat in het kader van de Wbp zomaar alles mag worden gedaan met de verzamelde gegevens. Elke keer als overwogen wordt om de gegevens te verwerken (inclusief raadplegen, wijzigen, etc.) moet worden afgewogen of professionals daartoe wel bevoegd zijn. Feitelijk worden professionals dus op het verkeerde been gezet. Te meer omdat in het maatschappelijk verkeer gebruikelijk is dat na het geven van toestemming de andere partij dan ook zijn gang mag gaan. In het geval van de Wbp is dat echter niet zo.

Uit de werkinstructie van Samen DOEN blijkt dat in sommige gevallen bepaalde gegevens wel worden opgeslagen, terwijl dat niet in het privacyprotocol wordt benoemd. In de werkwijzers en protocollen wordt niet beschreven dat persoonsgegevens moeten worden beoordeeld en eventueel aangepast na een triage moment.

Het risico op het bovenmatig uitvragen en registreren van (bijzondere) persoonsgegevens, waaronder gegevens over het justitiële en gezondheidsverleden van de betrokkene, is bij Samen DOEN en Wijkzorg voor de onderdelen ambulante zorg en dagbesteding groot. Het college is nog weinig sturend in het beperken van de gegevensverwerking tot het strikt noodzakelijke. De invulinstructie van de zelfredzaamheidmatrix leidt gemakkelijk tot het registreren van te veel, en dus niet noodzakelijke (bijzondere) persoonsgegevens. Bovendien moet de ZRM worden ingevuld om de effectiviteit van het programma Samen DOEN te kunnen monitoren. Een werkwijze ontbreekt dat na het uitvragen van de gegevens uit de zelfredzaamheidmatrix moet worden bepaald wat het probleem is en moet worden afgewogen welke gegevens daarvoor nog relevant zijn en moeten worden geregistreerd. Ook instructies om bij het maken van een (behandel)plan deze afweging nogmaals te maken hebben wij niet aangetroffen.

Het registreren van het burgerservicenummer (BSN) van anderen dan de betrokkene is bovenmatig en niet ter zake dienend. Een motivering in de protocollen ontbreekt waarom het BSN geregistreerd zou moeten worden, terwijl voor het bepalen van de mate van ondersteuning of hulpverlening het niet nodig is om ook het BSN van het sociale netwerk van de betrokkene te kennen. Bovendien biedt het BSN de mogelijkheid om persoonsgegevens te koppelen, waardoor de mogelijkheid wordt gecreëerd om de verkregen informatie voor een ander en niet verenigbaar doel te gebruiken dan waarvoor het was afgegeven. Zo zou informatie verkregen over een mantelzorger

(wijkzorg) ook door de gemeente gekoppeld kunnen worden met het dossier dat de gemeente heeft in het kader van de Participatiewet. Samen DOEN en Wijkzorg onderkennen dat de registratie van het BSN nummer van anderen dan de directe betrokkene bovenmatig is. Samen DOEN heeft het voornemen uitgesproken hier in de privacy roadshow en in de leerlijn extra aandacht aan te besteden. Wijkzorg heeft RIS-Wijkzorg sinds 1 januari 2016 zo aangepast dat de velden BSN en geboortedatum niet meer kan worden geregistreerd voor een ander dan de wettelijke vertegenwoordiger.[394] Dit laatste geldt alleen voor de module RIS-Wijkzorg, bij OKT en Samen DOEN is het nog wel mogelijk het BSN van een ander dan de betrokkene op te slaan.

5.5 Delen gegevens

Normen vanuit de Wbp – delen van gegevens
De verantwoordelijke hoeft de betrokkene slechts éénmalig te informeren dat hij gegevens aan derden verstrekt. Wanneer de verantwoordelijke de gegevens daarnaast ook nog met anderen wil delen moet hij daarover de betrokkene informeren.

Uit de preambule bij de privacyprotocollen OKT en Samen DOEN blijkt dat een adviseur alleen gegevens met collega's deelt als zij samenwerken om een specifieke hulpvraag te beantwoorden. Van te voren wordt aan de betrokkene uitgelegd met wie wordt samengewerkt. Als er een samenwerking nodig is met collega's die niet van te voren aan het huishouden meegedeeld zijn, wordt dat aan het huishouden gemeld en indien nodig wordt aan het huishouden toestemming gevraagd. Dit geldt ook voor collegiale toetsing[395] De adviseur verstrekt dan alleen die gegevens aan collega's die nodig zijn om te kunnen helpen. De adviseur legt gedurende de tijd dat hij het huishouden ondersteunt steeds uit wat hij doet, wanneer hij gegevens registreert en wanneer hij gegevens beschikbaar stelt aan deskundigen die betrokken zijn bij de hulpvraag. Voor het delen van (bijzondere) persoonsgegevens met derden geeft de betrokkene altijd vooraf toestemming.[396] Voor het opvragen van (bijzondere) persoonsgegevens van betrokkene bij een (externe) deskundige moet de betrokkene ook vooraf toestemming geven. De adviseur registreert de toestemming in RIS.[397]Als de adviseur een melding doet bij Veilig Thuis informeert hij het huishouden hierover, afhankelijk van de situatie doet hij dat vooraf of achteraf. Het vragen van toestemming blijft achterwege indien spoedzorg of -hulp buiten het wijkteam Samen DOEN, Ouder- en Kindteams of Wijkzorg moet worden ingeschakeld.[398]

Enigszins verwarrend is het dat het vanuit de Jeugdwet voor de hulpverlener verplicht is om toestemming te vragen aan de betrokkene om gegevens te mogen verwerken, terwijl deze toestemming niet de grondslag levert voor de gegevensverwerking zoals bedoeld in de Wbp (zie paragraaf 5.1.1). Het is dus feitelijk een extra

[394] Gemeente Amsterdam, Releasenote RIS-Wijkzorg versie 2.4,, februari 2016
[395] Zie ook Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 4.
[396] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 6; Privacyprotocol Wijkzorg art. 8 lid 4.
[397] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 5.
[398] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 9 lid 8; Privacyprotocol Wijkzorg art. 8 lid 6.

waarborg om zorgvuldig om te gaan met de verzamelde gegevens. Dit geldt ook als in het protocol aanvullende eisen worden gesteld rondom de cliënt.

De privacyprotocollen Samen DOEN en OKT maken het mogelijk dat (bijzondere) persoonsgegevens worden gedeeld zonder toestemming van de betrokkene.[399] De beschreven situaties waarin dit mogelijk is bevatten veel 'vage' termen, zoals 'spoedeisend', 'rechtstreeks betrokken bij hulpvraag', 'een belang dat zwaarder weegt dan de zwijgplicht'. Een nadere invulling van deze termen in een toelichting of een werkwijzer ontbreekt, waardoor het niveau van bescherming van privacy niet beoordeeld kan worden.

Hulpverlenende instellingen mogen (diagnose) gegevens delen met de gemeente ten behoeve van de facturatie en declaratie van geleverde zorg aan jongeren. Met terugwerkende kracht is vanaf 1 januari 2015 geregeld dat een ouder hiertegen bezwaar kan maken[400] Dit wordt ook wel de opt-out regeling genoemd. Wanneer een ouder gebruik maakt van de opt-out worden geen diagnostische gegevens op de factuur vermeld.[401] In de privacyprotocollen van Samen DOEN en OKT staat niets beschreven met betrekking tot het informeren van de betrokkene over deze opt-out regeling.

Op landelijk niveau speelt de discussie of domeinoverschrijdende gegevens-verwerking (van bijvoorbeeld Jeugdwet, Wmo en Participatiewet) binnen de samenwerkingsteams (zoals bijvoorbeeld Samen DOEN en OKT) is toegestaan. Zowel door het CBP als in de literatuur wordt gesteld dat dit niet is toegestaan omdat dit wettelijk niet is geregeld omdat deze wetten uitgaan van een gesloten regime van gegevensverstrekking.[402] De minister stelt zich op het standpunt dat op grond van artikel 9 Wbp domeinoverschrijdende gegevensverwerking mogelijk is omdat de doelen verenigbaar zijn. De keuze van het college van B en W voor de samen-werkingsteams van Samen DOEN en OKT duidt op de keuze voor een minder beschermende interpretatie van privacy ten voordeel van de hulpverlening.

Conclusies
De drie privacyprotocollen zijn op het punt van het delen van gegevens op hoofdlijnen in lijn met de Wbp.

Het college heeft gekozen voor domeinoverschrijdende gegevensverwerking (van bijvoorbeeld Jeugdwet, Wmo en Participatiewet) binnen de samenwerkingsteams van

Samen DOEN en OKT. Deze keuze duidt op een minder beschermende interpretatie van privacy ten voordeel van de hulpverlening. Bovendien is het mogelijk dat

[399] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 8 lid 2; Privacyprotocol Wijkzorg art. 7 lid 1.
[400] De Tijdelijke Ministeriële Regeling Jeugdwet is op 7 augustus 2015 in werking is getreden (met terugwerkende kracht tot 1 januari 2015)· Deze wet is bedoeld als overbrugging naar een definitieve regeling, die in de Veegwet VWS wordt opgenomen. De Veegwet zal begin 2016 van kracht gaan.
[401] Nieuwsbericht: CBP adviseert over regeling geheimhoudingsplicht Jeugdwet, CPB, 16 juli 2015
[402] W. Boor en A.M. van de Laar, Toestemming in de WMO 2015, Gemeentestem 2015/80.

(bijzondere) persoonsgegevens worden gedeeld zonder toestemming van de betrokkene.[403] Zonder een nadere concretisering van de vage situaties waarin dit mogelijk is, kan het niveau van bescherming van privacy niet beoordeeld worden.

5.6 Rechten van betrokkenen

Normen vanuit de Wbp
De verantwoordelijke zorgt er voor dat de betrokkene kan beschikken over de persoonsgegevens en de mogelijkheid heeft om gegevens te verbeteren, verwijderen of af te schermen.

Op grond van de privacyprotocollen kan het recht op inzage, correctie en vernietiging wordt uitgeoefend door:[404]

- de wettelijk vertegenwoordiger(s) als de betrokkene nog geen 12 jaar oud is;
- de wettelijke vertegenwoordiger(s) en de jongere beiden als de jongere al wel 12 maar nog geen 16 jaar oud is. Hierop geldt de uitzondering dat de jeugdige van 12 jaar of ouder zelf inzage in zijn dossier mag krijgen zonder dat zijn wettelijk vertegenwoordiger(s) er bij zijn;
- een persoon vanaf 16 jaar.

Is een jongere 12 jaar of ouder, maar naar het oordeel van de adviseur wilson-bekwaam, dan treedt of treden zijn wettelijke vertegenwoordiger(s) op namens hem.[405]

De adviseur kan inzage, correctie, of vernietiging beperken of weigeren indien dit niet in het belang van jeugdige of betrokkene is. Een gemotiveerd besluit daartoe wordt binnen 4 weken genomen. [406] Dit besluit wordt medegedeeld aan de verzoeker en vastgelegd in het dossier.[407] De beslissing tot verbetering, aanvulling, of verwijdering wordt bij Samen DOEN en OKT zo spoedig mogelijk uitgevoerd.[408] Over de snelheid van uitvoering wordt bij Wijkzorg geen uitspraak gedaan.[409]

[403] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 8 lid 2; Privacyprotocol Wijkzorg art. 7 lid 1.
[404] Privacyprotocol Samen DOEN art. 10 lid 2; privacyprotocol Ouder- en Kindteams art. 10 lid 1; privacyprotocol Wijkzorg art. 9 lid. 1. Tevens zijn in deze artikelen ook het recht van afschrift en het recht van een eigen verklaring geregeld.
[405] Privacyprotocol Samen DOEN art. 10 lid 3; privacyprotocol Ouder- en Kindteams art. 10 lid 2; privacyprotocol Wijkzorg art. 9 lid 2.
[406] Privacyprotocol Samen DOEN art. 11 lid2, 12 lid 2, privacyprotocol Ouder- en Kindteams art. 11 lid 2, privacyprotocol Wijkzorg art. 10 lid 2.
[407] Privacyprotocol Samen DOEN art. 10 lid 4; privacyprotocol Ouder- en Kindteams art. 10 lid 3; privacyprotocol Wijkzorg art. 9 lid 3.
[408] Privacyprotocol Samen DOEN art. 12 lid 3, privacyprotocol Ouder- en Kindteams art. 12 lid 3.
[409] Privacyprotocol Wijkzorg art. 10 lid 3, art 11 lid 4.

5.6.1 Inzagerecht

Iedere betrokkene heeft het recht om inzage in de door de verantwoordelijken over hem verwerkte persoonsgegevens te verzoeken. De adviseur [410] biedt namens de verantwoordelijke de betrokkene binnen vier weken inzage in en/of afschrift van de persoonsgegevens die over hem worden verwerkt, voor zover niet:[411]

- de privacy belangen van een derde[412] daardoor kunnen worden geschaad of
- de veiligheid van het kind in gevaar komt (geldt niet voor Wijkzorg)[413] of
- de adviseurs hun taak daardoor niet goed kunnen uitoefenen.[414]

De laatste uitzondering is te ruim en niet in lijn met de Wbp.[415]

Het recht op inzage betekent ook dat de betrokkene, als hij daarom vraagt, recht heeft op een afschrift (kopie) van de gegevens die hij mag inzien.[416]

5.6.2 Recht op correctie

De betrokkene kan de adviseur verzoeken persoonsgegevens te verbeteren, aan te vullen of te verwijderen indien deze feitelijk onjuist zijn, voor het doel van de verwerking onvolledig of niet ter zake dienend, dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek bevat de aan te brengen wijzigingen.[417]

De adviseur bericht binnen vier weken na ontvangst van het verzoek schriftelijk gemotiveerd op het verzoek. Ook een weigering is met redenen omkleed.[418]

De adviseur van Samen DOEN en het OKT draagt er zorg voor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd.[419]

---

[410] Aanvullend is bij Wijkzorg opgenomen dat de afhandeling van een verzoek om inzage in het dossier verloopt via de klanthouder. Deze informeert de verantwoordelijke van de andere betrokken partijen, die vervolgens zelfstandig verantwoordelijk zijn voor de afhandeling van het verzoek.(art 10 lid 3 Privacyprotocol Wijkzorg).

[411] In de Uniforme Werkwijze Samen DOEN in de buurt versie januari 2015, blz. 48 zijn aanvullend de volgende uitzonderingsgronden opgenomen:. voorkoming, opsporing en vervolging van strafbare feiten, de bescherming van de betrokkenen, de bescherming van de rechten en vrijheden van anderen.

[412] De derde kan zijn - maar niet uitsluitend - een van de ouders ingeval dat ouders gescheiden zijn en geen wettelijk gezag hebben of andere kinderen of familieleden in het huishouden. Het is mogelijk om bij dergelijke verzoeken de informatie die de privacy belangen van een derde kan schaden, af te schermen of weg te laten.

[413] Privacyprotocol Samen DOEN en Ouder- en Kindteams art. 11 lid 2.

[414] Privacyprotocol Samen DOEN en Ouder- en Kindteams art. 11 lid 2; privacyprotocol Wijkzorg art. 10 lid 2.

[415] Deze uitzonderingsgrond is niet in lijn met artikel 35 en 43 Wbp.

[416] Privacyprotocol Samen DOEN en Ouder- en Kindteams art. 11 lid 1; privacyprotocol Wijkzorg art. 10 lid 1.

[417] Privacyprotocol Samen DOEN en Ouder- en Kindteams art. 12 lid 1; privacyprotocol Wijkzorg art. 11 lid 1.

[418] Privacyprotocol Samen DOEN en Ouder- en Kindteams art. 12 lid 2; privacyprotocol Wijkzorg art. 11 lid 2.

[419] Privacyprotocol Samen DOEN en Ouder- en Kindteams art. 12 lid 3.

De afhandeling van een verzoek over het gehele dossier verloopt bij Wijkzorg via de klanthouder. Deze informeert de verantwoordelijken van de andere betrokken partijen, die vervolgens zelfstandig verantwoordelijk zijn voor het uitvoeren van het verzoek in het dossier dat onder hun beheer is. Een verzoek, gericht aan een specifieke partij, wordt door de betreffende partij afgehandeld.[420]

5.6.3 Recht op vernietiging

De betrokkene heeft het recht om de adviseur c.q. Wijkzorg te verzoeken de gegevens die op hem betrekking hebben te vernietigen. De adviseur c.q. Wijkzorg vernietigt de door hen bewaarde gegevens van betrokkene binnen drie maanden na een daartoe strekkend verzoek van betrokkene.[421]

Dit geldt niet voor zover het verzoek tot vernietiging gaat over informatie en documenten waarvan redelijkerwijs aannemelijk is dat de bewaring van aanmerkelijk belang is voor een ander dan betrokkene, alsmede voor zo ver het bepaalde bij of krachtens de wet zich tegen vernietiging verzet.[422]

Vernietiging van de gegevens vindt bij Samen DOEN en OKT plaats door deze uit het systeem te verwijderen of zo te anonimiseren dat de informatie niet tot personen herleidbare gegevens bevat. De bewerker draagt er zorg voor dat de vernietiging definitief is.[423] De vernietiging van gegevens van Wijkzorg vindt plaats door middel van afvoer door een daartoe gecertificeerd bedrijf of door anonimisering van de gegevens.[424]

5.6.4 Bewaartermijn

De wettelijke bewaartermijn van de dossiers is 15 jaar, daargelaten het artikel Recht op vernietiging uit het protocol. Deze termijn begint te lopen direct na het laatste contact met betrokkene(n) dat heeft geleid tot het sluiten van het dossier.[425]

Deze bewaartermijn kan worden verlengd als dat voor een zorgvuldige taakuitoefening van de wijkteams Samen DOEN, OKT en Wijkzorg noodzakelijk wordt geacht. Alleen de Programmamanager Samen DOEN of programmadirectie Ouder- en Kindteams mag dit besluit nemen. Dit besluit wordt gemotiveerd vastgelegd in het dossier van betrokkene.[426] Bij Wijkzorg wordt het besluit ook gemotiveerd vastgelegd in het dossier van betrokkene.[427] Er is niet beschreven wie dit besluit neemt.

---

[420] Privacyprotocol Wijkzorg art. 11 lid 3-4.

[421] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 15 lid. 1; Privacyprotocol Wijkzorg, art. 14 lid 1.

[422] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 15 lid. 2; Privacyprotocol Wijkzorg, art. 14 lid 2.

[423] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 15 lid 3.

[424] Privacyprotocol Wijkzorg, art. 14 lid 3.

[425] Privacyprotocol Samen DOEN en Wijkzorg, art. 21 lid 1; Privacyprotocol Ouder- en Kindteams, art. 22 lid 1.

[426] Privacyprotocol Samen DOEN, art. 21 lid 2; Privacyprotocol Ouder- en Kindteams, art. 22 lid 2.

[427] Privacyprotocol Wijkzorg, art. 21 lid 2.

5.6.5 Klachtenrecht

Totdat er een klachtenregeling Samen DOEN, Ouder- en Kindteams is vastgesteld, worden klachten afgehandeld volgens de klachtenregeling van de instelling bij wie de adviseur tegen wie de klacht gericht is, formeel in dienst is.[428] Samen DOEN heeft een eigen klachtencoördinator. De klachtencoördinator van rve Sociaal informeert de klachtencoördinator van Samen DOEN over klachten die binnenkomen over Samen DOEN, en vice versa.

Bij Wijkzorg kan een betrokkene een klacht over de omgang met zijn gegevens door een persoon of partij indienen bij de betreffende partij of bij de gemeente Amsterdam, team klachten.[429] Uitgangspunt voor klachten binnen Wijkzorg is dat klachten zo veel mogelijk worden afgehandeld op het niveau van de betrokken partij. De betrokken partij neemt de klacht in ontvangst en probeert de klacht als dat kan direct op te lossen door het gesprek aan te gaan met betrokkene. De afhandeling van de klacht verloopt, wanneer direct oplossen niet mogelijk is, volgens het proces zoals dat bij de partij of gemeente vastgelegd is.[430]

5.6.6 Rechtsbescherming

De betrokkene heeft het recht bezwaar te maken tegen een genomen besluit na het indienen van een verzoek tot inzage, correctie of verwijdering.[431] Bij Samen DOEN neemt de programmamanager binnen vier weken na datum van ontvangst van het verzoek een besluit en informeert de betrokkene tevens over de mogelijkheid voor het indienen van bezwaar. Voor Samen DOEN is beschreven tegen welke besluiten de betrokkene bezwaar kan maken. De betrokkene kan schriftelijk bezwaar maken bij het college van B en W binnen zes weken na de bekendmaking van het besluit.[432] Voor OKT en Wijkzorg staat niet beschreven of en hoe de cliënt bezwaar kan indienen tegen een dergelijk besluit.

5.6.7 Conclusie

De leeftijdsgrenzen voor inzage, correctie en vernietiging zijn in lijn met de Wbp en de Wet op de geneeskundige behandelingsovereenkomst (WGBO). In de laatste wet is geregeld hoe te handelen wanneer het kind een leeftijd heeft tussen de 12 en 16 jaar. Ook de termijn van vier weken waarbinnen het besluit moet worden genomen of aan het verzoek van inzage, correctie of vernietiging wordt voldaan, is overeenkomstig de Wbp. De protocollen regelen niet dat de verbeterde, aangevulde of verwijderde

[428] Privacyprotocol Samen DOEN en Ouder- en Kindteams, art. 16.

[429] Privacyprotocol Wijkzorg, art. 15 lid 1.

[430] Privacyprotocol Wijkzorg, art. 15 lid 2.

[431] Wbp, artikel 45. Indien een beslissing is genomen door een ander dan een bestuursorgaan, kan de belanghebbende zich tot de rechtbank wenden, Wbp, artikel 46.

[432] Werkwijze Samen DOEN in de buurt.

gegevens ook zo spoedig mogelijk worden gemeld aan derden waaraan al in een eerder stadium gegevens waren verstrekt.

Betrokkenen krijgen tijdig inzage in de over hen verwerkte persoonsgegevens. Niet is geregeld dat ze ook (gelijktijdig) worden geïnformeerd over het doel, de aard van de gegevens en van de ontvangers, alsmede over de herkomst van de gegevens.

Dat het recht op inzage geweigerd zou kunnen worden als de adviseurs hun taak daardoor niet goed kunnen uitoefenen is niet in lijn met de Wbp.

De bewaartermijn van 15 jaar is in lijn met de WGBO en de verlenging van deze termijn is in lijn met de Wbp. Wel is noodzakelijk dat ook Wijkzorg bepaalt wie bevoegd is om het besluit tot een langere bewaartermijn te nemen.

De Wbp regelt niets over het klachtrecht. Dit is wel geregeld in de Awb. De eerste stap – klagen bij de instelling die de klacht veroorzaakt waarbij de klachtenprocedure wordt gevolgd – is een juiste. Er ontbreekt in de privacyprotocollen de verdere werkwijze hoe te handelen als met de instelling niet tot overeenstemming kan worden gekomen.

In het privacyprotocol van OKT en Wijkzorg worden de betrokkenen niet gewezen op de mogelijkheid van rechtsbescherming.

5.7 Conclusie

Op veel punten voldoen de drie privacyprotocollen van Samen DOEN, het Ouder- en Kindteam (OKT) en Wijkzorg aan de Wbp. De doelen waarvoor de gegevens worden verzameld zijn welbepaald, gerechtvaardigd en duidelijk. Grondslagen voor de gegevensverwerking zijn benoemd. Positief is dat de beperking is opgelegd dat gegevens alleen worden verwerkt voor zo ver dat voor een goede hulpverlening aan betrokkene noodzakelijk is. De voorlichting aan en het informeren van de betrokkene, de geheimhouding, het delen van gegevens, de termijnen voor inzage, correctie, vernietiging en bewaring van persoonsgegevens zijn op hoofdlijnen allemaal in lijn met de Wbp. Daarmee is de privacy voor de betrokkene op die punten geborgd.

Toch is de privacy van betrokken niet volledig geborgd wanneer een ambtenaar of professional het protocol zou volgen. In de protocollen komt een expliciete afweging van het proportionaliteits- en subsidiariteitsbeginsel voor het verwerken van gegevens beperkt aan bod. Het protocol laat de ruimte om het burgerservicenummer (BSN) te registreren van anderen dan de betrokkene. Dit is bovenmatig en niet ter zake dienend. Vanaf 1 februari 2016 is het niet meer mogelijk om het BSN van een niet directe betrokkene in RIS-Wijkzorg te registreren. Voor RIS-Samen DOEN en RIS-OKT bestaat deze mogelijkheid nog wel.

Ten onrechte wordt in het protocol gesuggereerd dat een adviseur het recht op inzage kan weigeren als hij of zij zijn of haar taak daardoor niet zou kunnen uitoefenen. Dit is echter niet in lijn met de Wbp. Wanneer inzage in de persoonsgegevens wordt gegeven zou de adviseur de betrokkenen ook gelijktijdig moeten informeren over het doel en de aard van de gegevens(verwerking), wat de herkomst is van de gegevens en wie de gegevens nog meer gebruiken. In deze plicht voorzien de protocollen nog niet. Ook is nog niet geregeld dat als gegevens zijn gecorrigeerd, aangevuld of verwijderd, dit ook zo spoedig mogelijk worden gemeld aan derden waaraan al in eerder stadium gegevens waren verstrekt.

Een omissie bij de privacyprotocollen is dat we constateren dat zowel in de protocollen als in de werkwijzers niet wordt beschreven dat persoonsgegevens moeten worden beoordeeld en eventueel aangepast, na een triagemoment. Een omissie bij het protocol van Samen DOEN is dat uit de werkinstructie blijkt dat bepaalde gegevens wel worden opgeslagen terwijl dat niet in het protocol wordt benoemd.

Het privacyprotocol Wijkzorg schiet daarnaast te kort op het punt dat onvoldoende is geregeld dat persoonsgegevens alleen worden geregistreerd met toestemming van de betrokkene. In het privacyprotocollen OKT en Wijkzorg wordt niet gewezen op de mogelijkheid van een gang naar de rechter als betrokkene en verantwoordelijke er samen niet uitkomen (rechtsbescherming).

Ondanks dat is opgelegd dat gegevens alleen mogen worden verwerkt voor zover dat voor een goede hulpverlening aan betrokkene noodzakelijk is, is bij Samen DOEN en Wijkzorg voor de onderdelen ambulante zorg en dagbesteding het risico op het bovenmatig uitvragen en registreren van (bijzondere) persoonsgegevens groot. Gebruikers van RIS wordt aanbevolen om alle domeinen van de zelfredzaamheidsmatrix uit te vragen en te registreren, waaronder gegevens over het justitiële en gezondheidsverleden. Ook moet worden gemotiveerd waarom een bepaald leefgebied niet is uitgevraagd en verwerkt. Bij Samen DOEN dient de volledige ZRM ook ingevuld te worden om het programma te kunnen monitoren. In onze ogen is dit de omgekeerde wereld. De rekenkamer had op grond van de Wbp verwacht dat ambtenaren en professionals werden geïnstrueerd om terughoudend te zijn met het vastleggen van (bijzondere) persoonsgegevens en tijdens het proces meerdere malen zouden afwegen of gegevens nog noodzakelijk zijn voor de hulpverlening aan betrokkene.

Tot slot is het toezicht op de naleving van de Wbp door de samenwerkingsverbanden Samen DOEN, OKT en Wijkzorg nog onvoldoende geregeld. Afwijkingen van de Wbp kunnen daardoor zeer moeilijk worden geconstateerd en optreden in de handhavende sfeer is bijna onmogelijk. We constateren dat er geen specifieke voorlichtingsvormen zijn die speciaal gericht zijn op de groep van (licht) verstandelijk gehandicapten en de groep van mensen met zware psychische problemen. Positief is dat bij Samen DOEN door middel van trainingen aandacht wordt besteed aan het op

een begrijpelijke manier uitleggen van de folder aan (licht) verstandelijke gehandicapten.[433]

Voorgaande tekortkomingen zijn relatief eenvoudig te repareren. Maar ook wanneer deze aanpassingen zijn gemaakt zal het niet eenvoudig zijn om er voor te zorgen dat de privacy van de betrokkene in opzet goed wordt geborgd. Dit komt door dat de Wbp en protocollen ruime doelstellingen en vage bepalingen kennen die nader geconcretiseerd moeten worden om vast te kunnen stellen of gegevensverwerking plaatsvindt binnen de normen van de Wbp.[434] Vanwege de complexe domeinen van jeugd en zorg waarbij veel actoren, met verschillende expertise, zijn betrokken, zal het concretiseren geen eenvoudig opgave zijn. Belangrijk is dat het concretiseren een continue activiteit is die breed wordt gedragen door zowel het gemeentebestuur, de ambtelijke organisatie en samenwerkende partners. Het resultaat zou belegd kunnen worden in werkwijzers, die vervolgens in de protocollen van toepassing kunnen worden verklaard.

Deze concretisering biedt als voordeel dat bepaald kan worden welke opvatting het college van B en W heeft over privacy, een (erg) ruime of juist een beschermende opvatting. Dit biedt dan ook aanknopingspunten voor een bestuurlijke discussie. De keuze van het college om domeinoverschrijdende gegevensverwerking binnen samenwerkingsteams toe te staan, terwijl hier op landelijk niveau nog discussie over plaatsvindt, duidt op een mindere beschermende interpretatie van privacy ten voordeel van de hulpverlening.

[433] Feitelijk wederhoor, stedelijk directeur Sociaal, 16-02-2016

[434] Ook het CBP heeft bij de decentralisaties aangegeven dat de normen geoperationaliseerd moeten worden. Dit blijkt uit een brief van het CBP (Advies Privacytoets Jeugddomein) aan de Staatssecretaris van Volksgezondheid, Welzijn en Sport en de Staatssecretaris van Veiligheid en Justitie van 30 oktober 2014 waarin het CBP zich kritisch toonde over deze modellen en aanbevelingen. Het CBP merkt op dat de in de VNG-modellen en PIA opgenomen aanbevelingen een vrij algemeen karakter hebben en weinig oplossingsgericht en richtinggevend zijn. In het bijzonder wijst het CBP erop dat in de materiewetten geen grondslag is om de gemeentelijke taken op het gebied van jeugdzorg, maatschappelijke ondersteuning en werk en inkomen in onderlinge samenhang uit te voeren, zodat er geen wettelijke basis is voor een domeinbrede taakuitoefening.

6 Hoe wordt het proces rondom de burger uitgevoerd?

In het vorige hoofdstuk is beschreven aan welke privacyregels professionals en ambtenaren zijn gebonden wanneer ze hulp verlenen en welke rechten betrokkenen daarbij hebben. In dit hoofdstuk wordt de vijfde onderzoeksvraag beantwoord. De onderzoeksvraag luidt:

Hoe wordt het proces rondom de cliënt uitgevoerd en is dit in lijn met de Wbp en aanvullende regelgeving?

De algemene bevindingen zijn afkomstig uit een enquête onder RIS-gebruikers, waarin behalve Samen DOEN-leden ook medewerkers van OKT en Wijkzorg zijn benaderd (zie voor een toelichting op de enquête bijlage 4 en het bijlage boek).[435] Ook zijn de websites en folders van de verschillende samenwerkingsketens onderzocht om een beeld te krijgen van de voorlichtingsactiviteiten.

Er zijn verschillende redenen die de rekenkamer heeft doen besluiten om diepgaander onderzoek te doen naar Samen DOEN. Binnen de Samen DOEN-aanpak hebben professionals en ambtenaren te maken met multiprobleemsituaties waarbij zowel interne als externe organisaties zijn betrokken die noodzakelijkerwijs intensief informatie moeten delen. Ook functioneert Samen DOEN al langere tijd (sinds 2011) en heeft daarmee ruime ervaring met het werken in multidisciplinair teamverband en het werken met RIS.

De aanpak en werkwijze van de Samen DOEN-teams en de ervaringen die de team-leden hebben met gegevensverwerking is op twee manieren onderzocht. Er is gebruik gemaakt van een groepsgesprek met 10 medewerkers van Samen DOEN (zie bijlage 5) en aan de enquête hebben 86 medewerkers van Samen DOEN deelgenomen. Deze twee groepen samen worden aangeduid als de *focusgroep*.

In paragraaf 6.1 wordt eerst wat achtergrondinformatie over Samen DOEN gegeven. Ter verduidelijking wordt door middel van een door ons geconstrueerde, fictieve casus beschreven hoe de procedure voor een cliënt bij Samen DOEN verloopt en op welke momenten er beslissingen rondom privacy en gegevensverwerking moeten worden genomen.

In het verdere hoofdstuk wordt aandacht besteed aan verschillende aandachtspunten rondom gegevensregistratie en gegevensdeling. We starten met de vraag in welke mate de respondenten kennis hebben van de privacyregelgeving en de mogelijkheden om kennis te verwerven en uit te breiden (zie paragraaf 5.2). In paragraaf 6.3 gaan we

[435] De 552 respondenten die de enquête hebben ingevuld bestonden uit 436 respondenten van de RIS-modules Samen DOEN, OKT en Wijkzorg. De overige 116 respondenten werken met andere RIS-modules of maken geen gebruik (meer) van RIS.

in op de manier waarop de voorlichting via de website, folder en privacyprotocol geregeld is (zie paragraaf 5.3). In paragraaf 6.4 en 6.5 behandelen we op welke wijze gegevensverwerking in de praktijk wordt uitgevoerd. In de paragraaf 6.4 staat de registratie van gegevens centraal (zie paragraaf 5.4) en in paragraaf 6.5 het delen van gegevens (zie paragraaf 5.5). De rechten van de betrokkene, waaronder het inzagerecht en het recht op correctie komen in paragraaf 6.6 aan de orde (zie paragraaf 5.6). We sluiten dit hoofdstuk af met een conclusie over de vraag hoe de afspraken uit het vorige hoofdstuk in de praktijk uitpakken, worden ervaren door professionals en ambtenaren en of in lijn wordt gehandeld met de Wet bescherming persoonsgegevens (Wbp) en de privacyprotocollen.

6.1 Samen Doen

In deze paragraaf zal kort worden ingegaan op wat Samen DOEN is. Vervolgens zullen de verschillende momenten van gegevensverwerking in het proces van Samen DOEN belicht worden door middel van een fictieve casus.

6.1.1 Achtergrondinformatie Samen DOEN

Samen DOEN is een initiatief van gemeente Amsterdam en is gestart in 2011.
De 22 wijkteams van Samen DOEN richten zich op ondersteuning van kwetsbare huishoudens waarin sprake is van meervoudige problemen (zoals armoede, wonen, schulden, werk, opvoeding en licht verstandelijke beperkingen) bij gezinsleden die niet of in beperkte mate zelfredzaam zijn. De teams werken vanuit het principe één huishouden, één plan en één regisseur en stimuleren de zelfredzaamheid van de betrokkenen. De Samen DOEN-teams lossen problemen zoveel mogelijk zelf op, bevorderen zelfregie (eigen kracht) of zetten vroegtijdig maatschappelijke steunsystemen in. Ze bieden structuur in het alledaagse (over)leven en voorkomen dat problemen zich opstapelen of escaleren.

De gemeente is verantwoordelijk voor de organisatie van de teams en voor de leerlijn waarin de professionals ondersteuning en training krijgen. De teams zijn samengesteld uit een teamleider, een teamassistent (beiden in dienst van de gemeente) en een aantal teamleden die werkzaam zijn bij diverse zorg- en welzijnsinstellingen. Aanmeldingen komen via de teamassistent binnen, waarna de teamleider beoordeelt of de cliënt binnen de doelgroep valt. Als dat het geval is, nemen één of twee professionals uit het team de casus over, gaan ze met de cliënt in gesprek en stellen ze een integraal behandelplan op. Een team komt ongeveer één keer in de twee weken bij elkaar voor casuïstiekbesprekingen en overleg.[436]

[436] Ontleend aan College van B en W, Notitie *'Toekomst van de wijkteams in Amsterdam'*, 2014, p. 3 en http://www.amsterdam.nl/zorg-welzijn/programma-samen-0/programma-samen/.

6.1.2 Casus: hoe verloopt de procedure bij Samen DOEN voor de cliënt?

Een Amsterdammer doorloopt een uitgebreid proces wanneer hij of zij zich aanmeldt, of wordt aangemeld, bij Samen DOEN. Om het huishouden zo goed mogelijk te kunnen helpen, worden tijdens dit proces (bijzondere) persoonsgegevens vastgelegd en gedeeld. De registratie van gegevens begint op het moment dat het huishouden is aangemeld bij Samen DOEN en eindigt in principe bij het vernietigen van gegevens, 15 jaar na het sluiten van het dossier.

Om bovenstaande procedure te verhelderen is een door ons geconstrueerde, fictieve casus geschetst zoals die zich binnen Samen DOEN zou kunnen voordoen. [437] Het is een voorbeeld van hoe de processen bij Samen DOEN in theorie zouden moeten verlopen (volgens het privacyprotocol).

Een inwoonster van de gemeente Amsterdam, mrvrouw De Jong, gaat al jaren gebukt onder grote schulden en een alcoholverslaving. De situatie wordt bemoeilijkt door stemmings-wisselingen ten gevolge van een persoonlijkheidsstoornis. Ook haar twee kinderen hebben last van de onstabiele thuissituatie. Zo spijbelen ze regelmatig van school en is er geen geld voor de sportschool of ander vermaak. Hierdoor zitten ze veel thuis en hangen ze rond op straat. Mw. De Jong loopt tegen verscheidene problemen aan in het opvoeden van haar twee kinderen. Na een tip van haar buurvrouw vervoegt ze zich voor opvoedhulp bij het Ouder- en kindteam. Het OKT merkt al snel dat mevrouw. De Jong niet alleen problemen heeft met de kinderen, maar problemen heeft op meerdere terreinen. Het OKT neemt contact op met Samen DOEN om de casus van mevrouw De Jong over te dragen.

Nadat de hulpverlener van het OKT hiervoor toestemming heeft gevraagd aan mevrouw. De Jong, en zij heeft toestemming gegeven, meldt zij mevrouw De Jong aan bij Samen DOEN via het aanmeldformulier van Samen DOEN. Het aanmeldformulier bestaat uit de gegevens van de aanmelder, het adres en telefoonnummer van het huishouden, de basisgegevens van de leden van het gezin (ieders naam, rol in het gezin, geslacht, geboortedatum en BSN-nummer), een overzicht van de situatie per leefgebied in de zelfredzaamheidmatrix (ZRM), de betrokkenen, de reden van de aanmelding en eventuele zorgen rondom veiligheid en zo ja, voor wie. Dit aanmeldformulier komt terecht bij de teamassistente van het Samen DOEN team. De teamassistente beoordeelt de aanmelding door vast te stellen of het gezin tot de doelgroep behoort en een regiecheck uit te voeren. Dit laatste om te voorkomen dat het gezin door meerdere hulpverleners, los van elkaar, wordt geholpen. Omdat evrouw. De Jong tot de doelgroep behoort (ze heeft immers problemen op meerdere leefgebieden) en er geen regie blijkt te zijn op haar dossier maakt de teamassistente een dossier aan in het registratiesysteem van Samen DOEN (verder: RIS). Door de teamassistente wordt één dossier aangemaakt waarin de informatie van zowel mevrouw De Jong als haar twee kinderen staat. Vervolgens wordt mevrouw De Jong toegekend aan een teamlid van Samen DOEN. Mevrouw De Jong krijgt een brief van het teamlid met een verzoek om contact op te nemen.

[437] Op basis van de Uniforme Werkwijze Samen DOEN in de buurt.

Het verantwoordelijke teamlid van Samen DOEN nodigt haar uit voor een gesprek, het zogenaamde keukentafelgesprek. Het teamlid inventariseert samen met mevrouw. De Jong de situatie en of ondersteuning door het buurtteam mogelijk en gewenst is. Ook legt het teamlid uit wat de visie en werkwijze van Samen DOEN is. Zij krijgt een folder overhandigd waarin informatie staat over de werkwijze van Samen DOEN en de manier waarop Samen DOEN met persoonsgegevens omgaat. Gezamenlijk wordt besloten door te gaan met de ondersteuning. Omdat mevrouw De Jong opvoed- en opgroeiondersteuning nodig heeft, wordt haar toestemming gevraagd voor de registratie van (bijzondere) persoonsgegevens[438]. Na akkoord wordt het dossier van mevrouw De Jong aangevuld met in elk geval informatie over haar sociale netwerk, de nul situatie van de ZRM (volledig ingevuld) en de jeugdzorgproblematiek.

Nu de beginsituatie helder is wordt door het teamlid en het gezin besloten een plan voor ondersteuning op te stellen. De doelstelling en acties van het plan worden in het dossier in RIS vastgelegd. Mevrouw De Jong heeft een buurvrouw die haar af en toe zou kunnen helpen met de financiën. Nadat de buurvrouw hier mondeling toestemming voor heeft gegeven, worden ook haar naam, adres en telefoonnummer in RIS genoteerd. De eerste paar maanden na de start van ondersteuning is regelmatig contact tussen het teamlid van Samen DOEN en mw. De Jong. Deze contactmomenten worden geregistreerd in RIS.

De dochter van memvrouw De Jong is benieuwd welke gegevens er van haar worden opgeslagen in het digitale dossier. Ze doet een verzoek tot inzage bij de contactpersoon van Samen DOEN. Het teamlid laat haar een uitdraai zien van het RIS systeem, waarbij om privacy redenen de gegevens van haar moeder en broer zwart zijn gemarkeerd. De dochter is niet gerustgesteld en wil een formeel verzoek tot inzage indienen. De hulpverlener vertelt haar dat ze dit schriftelijk moet indienen bij de programmamanager van Samen DOEN. Na een maand ontvangt ze een overzicht van de verwerkte gegevens, een omschrijving van de doeleinden van de verwerking, de soorten gegevens waarop de verwerking betrekking heeft, de (categorieën van) ontvangers en geanonimiseerde informatie over de herkomst van de gegevens, voor zover niet direct van de betrokkene verkregen. Ze wordt ook geïnformeerd over de voorwaarden voor het indienen van een eventueel verzoek tot verbetering, aanvulling, verwijdering of afscherming van gegevens en het indienen van een bezwaar.

De dochter vindt na het lezen van de dossierinformatie dat sommige gegevens niet kloppen. Ze wil deze informatie laten verwijderen uit het dossier. De buurtteammedewerker vertelt haar dat ze schriftelijk een verzoek tot vernietiging in kan dienen bij de programmamanager. De programmamanager legt het verzoek bij een aangewezen medewerker, de behandelaar. De behandelaar heeft vier weken om te bepalen of aan het verzoek kan worden voldaan. De dochter krijgt na 4 weken te horen dat niet aan haar verzoek tot vernietiging kan worden voldaan. In het besluit wordt ze gewezen op de mogelijkheid tot het indienen van bezwaar. Het gezin wordt verder naar alle tevredenheid geholpen en na 2 jaar is de zelfredzaamheid van mevrouw De Jong en haar gezin zodanig verbeterd dat de hulpverlening kan worden stopgezet. Het dossier wordt afgesloten door de laatste processtap Afsluiten in RIS volledig in te vullen. Twee jaar na het laatste contactmoment wordt het dossier automatisch gearchiveerd in RIS. Het dossier wordt tot 15 jaar na het laatste contactmoment bewaard.

---

[438] Artikel 9, lid 2, privacy protocol Samen DOEN

De fictieve casus laat zien dat er verschillende momenten zijn waarop er gegevens van de cliënt worden opgeslagen of gedeeld. Aandachtpunten zijn de kennis van privacyregelgeving, de voorlichtingsactiviteiten, het registreren van gegevens het delen van gegevens en de rechten van de betrokkene. In de volgende paragrafen gaan we dieper in op de gegevensverwerking in de praktijk. Hiervoor zullen we per aandachtspunt eerst ingaan op de manier waarop professionals van zowel OKT, Wijkzorg en Samen DOEN bij de verschillende aandachtspunten in de praktijk handelen. Bij elk aandachtspunt zal vervolgens met behulp van de inbreng van de professionals van Samen DOEN in het groepsgesprek dieper worden ingezoomd op de verschillende aandachtspunten.

6.2 Kennis van privacyregelgeving

Het uitgangspunt is dat professionals en ambtenaren het privacyprotocol bij het handelen in acht nemen. Dit vereist wel kennis van dit protocol en de Uniforme Werkwijze (zie paragraaf 4.4.3) of de daaraan ten grondslag liggende regels over privacy (bijv. de Wbp, WGBO). Alleen met deze kennis kunnen belangen tussen privacy en gegevensverwerking goed worden afgewogen en kan rechtmatig worden gehandeld. Om te kunnen spreken van een goede kennis van privacyregelgeving onder professionals en ambtenaren vinden wij dat uit de enquête moet blijken dat minimaal tweederde van de ondervraagden aangeeft voldoende kennis hebben. Dit is het geval, maar er zijn ook aandachtpunten.

De professionals en ambtenaren van OKT, Wijkzorg en Samen DOEN geven aan dat hun eigen kennis over de privacyregels goed op orde is. Ongeveer 60% van de ondervraagden is van mening dat ze zelf genoeg kennis hebben van de privacyregels om op een goede manier met privacygevoelige gegevens om te gaan. Toch zijn de privacyregels niet voor iedereen volledig duidelijk. Circa een kwart van de respondenten vindt de privacyregelgeving voor meerdere uitleg vatbaar en daardoor onduidelijk. Ook is een derde van mening dat er te veel privacyregels zijn waardoor het geheel complex is. Uit de toelichting op de vragen blijkt niet iedereen altijd op de hoogte te zijn van de privacyregelgeving (zie tekstkader).

> *Ik merk door het invullen van deze enquête dat ik onvoldoende op de hoogte ben van het privacyreglement*

Focusgroep Samen DOEN
De deelnemers van Samen DOEN geven aan dat de privacyregelgeving continu aandacht vraagt. Als wordt doorgevraagd in het groepsgesprek blijkt dat details soms niet bij iedereen bekend zijn, zoals de uitzonderingsgronden voor gegevensdeling zonder toestemming van de betrokkene met derden. Als het bijvoorbeeld gaat om kind-onveiligheid dan wordt soms uit voorzichtigheid besloten om informatie niet te delen, terwijl dat in die gevallen wel mag in het belang van het kind. Als niet iedereen daarover hetzelfde denkt, dan

kan dat leiden dat tot problemen. Ook komt naar voren dat de teamleiders wat meer dan de teamleden teruggrijpen op het privacyprotocol. Teamleden volgen eerder de uniforme werkwijze en vragen informatie aan collega's. Bij het doorvragen blijkt dat privacy wel is verwerkt in de algemene leerlijn, maar nog geen aparte module is waar specifiek wordt ingegaan op de privacyregels en de belangenafweging die soms moet worden gemaakt bij het toepassen daarvan.

6.2.1 Conclusie

De rekenkamer vindt kennis van de Wbp een randvoorwaarde voor een goede taakuitoefening door professionals en ambtenaren om overeenkomstig de Wbp te kunnen handelen (zie ook paragraaf 5.2). Uit de bevindingen blijkt dat de meeste professionals en ambtenaren vinden dat hun eigen kennis van privacyregelgeving goed op orde is. Wel dient opgemerkt te worden dat een derde van de professionals aangeeft de regels te complex te vinden. Nieuwe medewerkers worden niet structureel geïnformeerd over het privacyprotocol. Ook in de leerlijn wordt nog onvoldoende aandacht besteed aan kennis over en het omgaan met de rechten van betrokkene.

6.3 Voorlichting via de website, folders en het privacyprotocol

In de privacyprotocollen van Samen DOEN, Wijkzorg en OKT staat expliciet beschreven dat de professional uitlegt hoe moet worden omgegaan met persoonsgegevens, welke rechten de betrokkene heeft en dat betrokkene actief moet worden geïnformeerd. Dit gebeurt voorafgaand aan of in het eerste gesprek. Burgers kunnen informatie vinden over hun privacyrechten op de website, via folders en in het privacyprotocol.

6.3.1 Website

Op de website van de gemeente is onder de dienst Ruimte en Wonen een pagina met informatie voor burgers rondom privacy te vinden: 'de gemeente en uw privacy'.[439] Op deze pagina wordt informatie gegeven over de manier waarop de gemeente Amsterdam omgaat met persoonsgegevens, de informatieplicht die de gemeente heeft op basis van de Wbp, de beveiliging van de systemen waarin de gegevens staan opgeslagen en het recht van de burger om kennis te nemen van zijn gegevens en deze te corrigeren. Vervolgens wordt de burger verwezen naar de websites www.cbpweb.nl of www.mijnprivacy.nl. Ook op de website van de GGD Amsterdam is informatie te vinden over de jeugdgezondheidszorg (JGZ) en privacy.[440] Algemene informatie over privacy op de website van de gemeente Amsterdam is verspreid over de website en voor de burger moeilijk vindbaar. De informatie sluit aan bij een aantal eisen die de Wbp stelt aan gegevensverwerking (de informatieplicht van de

[439] https://www.amsterdam.nl/gemeente/organisatie/ruimte-economie/wonen/gemeente-privacy/
[440] http://www.ggd.amsterdam.nl/jeugd-0/jgz-privacy/

gemeente, de passende technische en organisatorische beveiligingsmaatregelen die de gemeente stelt en het recht op kennisname en correctie). Samen DOEN, OKT en Wijkzorg beschikken daarnaast ook over een eigen website.

Samen DOEN
Op de pagina van Samen DOEN op de gemeentelijke website wordt de cliënt geïnformeerd over zijn of haar rechten: het recht op inzage, wijziging en vernietiging. Ook staat beschreven dat de gemeente zich bij het verwerken van persoonsgegevens aan de wet houdt, alleen gegevens worden opgeslagen die nodig zijn, aangeeft wie er in het dossier kunnen, dat de professionals geheimhoudingsplicht hebben en na welke termijn het dossier wordt afgesloten. De informatie die op de website van Samen DOEN wordt gegeven is in lijn met de Wbp. Daarnaast is op de website van Samen DOEN de *folder Samen DOEN* beschikbaar gesteld, waarin ook op het onderwerp privacy wordt ingegaan.[441] Op de website is het privacyprotocol van Samen DOEN niet beschikbaar.

OKT
De Ouder- en Kindteams beschikken over een eigen website waarop informatie te vinden is over de manier waarop de Ouder- en Kind teams omgaan met privacy.[442] Daarbij wordt ingegaan op het digitaal dossier, delen van informatie, toestemming, uitzonderingen op de toestemming, verwijzingen en vragen over klachten en privacy. Tevens komt het recht van inzage en verzoek tot wijzigen gegevens aan bod. De gegeven informatie sluit aan bij de Wbp.

Wijkzorg
Op de website van de gemeente wordt de burger geïnformeerd over maatregelen voor het waarborgen van de privacy van betrokkenen van Wijkzorg. Er worden een aantal maatregelen genoemd die zijn genomen om het privacyrisico bij het ondertekenen van het ondersteuningsplan zo klein mogelijk te houden.[443] Daarnaast kan de folder Wijkzorg worden gedownload.[444] Hierin wordt summier ingegaan op privacy. Voor professionals is er een website *Wegwijs in de Wmo*, met alle relevante informatie en documenten, zoals factsheets, het stedelijk kader Wijkzorg en werkinstructies. Daarnaast is er een aparte nieuwsbrief voor Wijkzorg. Deze verschijnt sinds maart 2015 één keer per maand.

[441] https://www.amsterdam.nl/zorg-welzijn/programma-samen-0/samen/
[442] http://oktamsterdam.nl/privacy/
[443] https://www.amsterdam.nl/gemeente/organisatie/sociaal/onderwijs-jeugd-zorg/zorg-wmo-beleid/wegwijs-wmo/nieuws-wegwijs-wmo/2014/wijkzorg-privacy/
[444] https://www.amsterdam.nl/zorg-welzijn/zorg-ouderen/wijkzorg/

6.3.2 Folder

Samen DOEN, Wijkzorg en OKT informeren de burger ook via een folder.

Samen DOEN

Voor Samen DOEN is een folder beschikbaar die tijdens het eerste contactmoment met de burger wordt meegegeven.[445] Onderwerpen rondom privacy waar de cliënt via de folder over wordt geïnformeerd zijn: informatie over de manier waarop Samen DOEN omgaat met persoonlijke gegevens, recht op kennisneming en correctie, wie toegang hebben tot het dossier en de geheimhoudingsplicht van de professionals. Ook staat beschreven hoe de cliënt een klacht zou kunnen indienen. Informatie over het delen van gegevens ontbreekt.

OKT

Voor OKT is een factsheet beschikbaar om ouders en professionals te informeren over privacy. De informatie in deze factsheet komt overeen met de informatie op de website.[446] De Jeugdgezondheidszorg heeft, als onderdeel van de Ouder- en Kind-teams, een folderlijn opgesteld. Zo is er een folder voor ouders beschikbaar. In de folder komt privacy aan de orde. In de folder wordt de ouder geïnformeerd over welke gegevens van het kind in het digitaal dossier worden opgenomen. Ook wordt de ouder uitgebreid geïnformeerd over het delen van gegevens. De ouder wordt erop gewezen dat de professional zorgvuldig omgaat met de gegevens en dat het dossier goed beveiligd is. Voor meer informatie over privacy wordt de ouder verwezen naar de website www.oktamsterdam.nl.

Bij zowel Samen DOEN als OKT worden ouders niet actief via de website en folder geïnformeerd over de mogelijkheid gebruik te maken van de opt-out regeling (Zie paragraaf 5.5).

Wijkzorg

Bij Wijkzorg wordt de burger via twee formulieren geïnformeerd over privacy. Door middel van de folder Wijkzorg en de voorbeeldbrief *cliënt persoonlijke gegevens Wijkzorg* (oktober 2015).[447] In de folder van Wijkzorg wordt de betrokkene erop gewezen dat de klanthouder alleen gegevens deelt met andere hulpverleners wanneer de betrokkene toestemming geeft. Sinds 1 februari 2016 is het systeem RIS zo aangepast, dat bij printen van het ondersteuningsplan, de brief automatisch wordt meegeprint. Op deze manier is bewerkstelligd dat de cliënt direct met het ondersteuningsplan ook de brief over privacy meekrijgt. De informatie in de brief is in lijn met de Wbp en biedt antwoorden op de meest voorkomende vragen over privacy.

---

[445] Interview 26-10-2015

[446] http://oktamsterdam.nl/privacy/

[447] https://www.amsterdam.nl/gemeente/organisatie/sociaal/onderwijs-jeugd-zorg/wegwijs-in-de-wmo/wmo-docs-voorziening/wijkzorg/

6.3.3 Privacyprotocol

Het privacyprotocol van Samen DOEN, OKT en Wijkzorg bevat een preambule. Hierin zijn de rechten van de betrokkene en de werkwijze van de professional helder beschreven. Tevens is nader ingegaan op de werkwijze bij het registreren en het uitwisselen van persoonsgegevens. Vanuit het perspectief van voorlichting is dit nuttig voor de betrokkene om hier kennis van te nemen. Vanuit de ambtelijke organisatie is benadrukt dat de preambule speciaal vanuit dit oogpunt is opgesteld.[448] De privacyprotocollen van Samen DOEN en OKT zijn in januari 2016 echter nog niet (eenvoudig) toegankelijk voor de betrokkene.[449]

6.3.4 Conclusie

Gezien de uitgangspunten van de VNG wordt de betrokkene in opzet via meerdere kanalen geïnformeerd. Wel blijken de folder nog niet altijd te worden meegegeven door de professionals. [450] Ook de informatie per kanaal kan worden uitgebreid. Dit is bij OKT het beste geregeld, daar wordt de cliënt zowel via een folder als via de website volledig geïnformeerd.

De website van Samen DOEN en Wijkzorg is vanuit het oogpunt van voorlichting niet volledig. Bij Samen DOEN, OKT en Wijkzorg is een folder aanwezig waarin de betrokkene wordt geïnformeerd. Wijkzorg heeft aanvullend een informatieve brief beschikbaar. De informatie die in de folder wordt gegeven is over het algemeen in lijn met de Wbp. Aandachtspunten zijn de geringe hoeveelheid informatie in de folder van Wijkzorg. Dit wordt deels ondervangen door de brief die Wijkzorg beschikbaar stelt. Deze wordt sinds 1 februari 2016 automatisch met het ondersteuningsplan meegegeven aan de burger.[451] In de folder van Samen DOEN mist informatie over het delen van gegevens. De privacyprotocollen van Samen DOEN en OKT zijn op 16 januari 2016 nog niet beschikbaar voor de betrokkene. Op dit punt is van een actieve vorm van voorlichting daarom nog geen sprake.

6.4 Registreren van gegevens

Vraagt de betrokkene ondersteuning of hulpverlening aan, dan worden in veel gevallen (bijzondere) persoonsgegevens over de betrokkene opgeslagen. Het is daarbij van belang dat de betrokkene daarover goed wordt geïnformeerd en daar in sommige gevallen zelfs toestemming voor geeft.

---

[448] Interview, 09-11-2015

[449] Het privacyprotocol Wijkzorg is te downloaden via https://www.amsterdam.nl/gemeente/organisatie/sociaal/onderwijs-jeugd-zorg/wegwijs-in-de-wmo/nieuwsbrief-wegwijs/wegwijs-wmo-44/.

[450] Interview rekenkamer, 10 november 2015.

[451] Interview rekenkamer, 10 november 2015.

6.4.1 Informeren betrokkene over registratie van gegevens

Uit de Wbp volgt dat de betrokkene geïnformeerd moet worden over het doel van de registratie. We mogen ervan uit gaan dat professionals en ambtenaren dit ook doen. Uit de enquête blijkt dat een meerderheid van de professionals en ambtenaren de betrokkene inderdaad informeert. Zij geven aan vaak (22,9%) tot altijd (56,2%) de betrokkene te informeren over het doel van de registratie. Echter is er ook een kleine groep die aangeeft soms (11,6%) tot nooit (7,7%) over het doel te informeren.

Focusgroep Samen DOEN

De focusgroep onderstreept het belang van het informeren van de betrokkene. Het beeld leeft bij hen dat registreren van gegevens 'vanzelfsprekend' is. De focusgroep geeft aan dat informeren van de cliënt over het doel van de gegevensregistratie niet altijd wordt gedaan. Dat heeft te maken met de specifieke doelgroep van Samen DOEN: de multiprobleemhuishoudens. De betrokkenen zouden achterdochtig kunnen worden als zij worden geïnformeerd over het doel van registratie. De professional maakt daarom in de praktijk een inschatting of de betrokkene het zal begrijpen of van de informatie bang, onrustig of achterdochtig zal worden. Ook wordt de betrokkene soms niet geïnformeerd over het doel omdat er onvoldoende tijd is. Een van de Samen DOEN-medewerkers gaf daarbij als voorbeeld: *"Ik vertel niet dat de gemeente ook de gegevens anoniem kan gebruiken."* Ten slotte kwam in het groepsgesprek de vraag naar voren of iedereen wel het informatieformulier aan de betrokkene meegeeft. Aangegeven wordt dat hier geen gegevens over bestaan.

6.4.2 Toestemming betrokkene voor het registreren van gegevens

Het vragen van toestemming voor het registreren van gegevens is volgens de protocollen van Samen DOEN en OKT slechts in bepaalde situaties voorgeschreven, zijnde ij opvoed- en opgroeiondersteuning, ondersteuning op grond van de Wet Publieke gezondheid en bij jeugdhulp (WGBO). Voor Wijkzorg is er geen verplichting voor het vragen van toestemming.

Ondanks dat het niet verplicht is, geven de professionals en ambtenaren van OKT, Wijkzorg en Samen DOEN aan dat ze vaak (16,5%) tot altijd (60,9%) toestemming vragen wanneer ze gegevens registreren. Opvallend is dat vaak toestemming wordt gevraagd terwijl dit volgens de privacyprotocollen meestal niet nodig is. Een verklaring hiervoor kan zijn dat het tot oktober 2015 in alle situaties verplicht was toestemming te vragen voor de registratie van persoonsgegevens.

De meeste professionals en ambtenaren (78,4%) geven aan mondeling toestemming te vragen. Degenen die schriftelijk om toestemming vragen doen dit vaak (19,7%) tot altijd (57,7%) met een toestemmingsformulier. Professionals zijn niet verplicht betrokkenen een formulier te laten tekenen wanneer het gaat om het registreren van gegevens.[452]

[452] Gesprekverslag, 26-10-2015

Vastleggen van gegevens wanneer betrokkene niet instemt
Wanneer de betrokkene niet instemt met de gegevensverwerking of aangeeft dat persoonsgegevens niet mogen worden vastgelegd, dan heeft de professional de mogelijkheid de hulpverlening te stoppen. Eén op de twintig professionals geeft aan de hulpverlening in die situatie te beëindigen of niet te starten, het merendeel blijft hulp verlenen als de betrokkene geen toestemming geeft. Zij doen dit zonder persoonsgegevens te verwerken in RIS (11%), door alleen beperkte gegevens in RIS in te voeren (14%) of door aantekeningen vast te leggen buiten RIS om (17%). Een derde (35%) geeft aan eerst met het team te overleggen voordat ze bepalen wat ze doen. Ten slotte is er een deel (17%) die niet weet wat ze zouden doen in deze situatie.

Focusgroep Samen DOEN
Ook uit het groepsgesprek met Samen DOEN bleek dat het toestemmingsformulier voor het registreren van persoonlijke gegevens in het RIS-systeem is komen te vervallen. Registratie wordt nu als een wezenlijk onderdeel van de hulpverlening gezien, waardoor gegevens kunnen worden opgeslagen zonder dat toestemming wordt gevraagd of verkregen. Een vertegenwoordiger van de gemeente zegt hierover: "*Er mag nu wel worden geregistreerd zonder expliciete toestemming van de cliënt, dit hoort immers bij het verlenen van hulp en voor het verlenen van hulp is toestemming nodig. Door als cliënt akkoord te gaan met de hulpverlening wordt daardoor ook akkoord gegeven voor het registreren van gegevens*". Een andere deelnemer vindt dit geen goede ontwikkeling: "*Binnen Samen DOEN heeft er een verandering plaatsgevonden, eerst was er schriftelijk toestemming van het gezin en een handtekening nodig waardoor het altijd onderwerp van gesprek was. Nu blijkt mondelinge toestemming te volstaan, waardoor niet altijd gegarandeerd is waarvoor en voor wie en met wie contact opgenomen mag/kan worden.*"

Bij Samen DOEN geeft één op de vijf respondenten in de enquête aan (bijna) nooit toestemming te vragen voor het registreren van gegevens in RIS. Afhankelijk van de taak die wordt verricht is toestemming vragen al dan niet noodzakelijk. Er zijn meerdere redenen waarom toestemming niet wordt gevraagd. Gegevens zouden maar weinig gevoelig zijn of soms wordt het simpelweg vergeten. Wel wordt aangegeven dat het vragen van toestemming niet altijd goed doordringt bij de betrokkene: "*In de doelgroep van Samen DOEN dringt het bij een substantieel aantal mensen niet door. Dat is een groot knelpunt. Dat gegeven leidt nadrukkelijk niet tot nonchalance. Het is wel belangrijk om te zoeken naar manieren om het probleem op te lossen*."

Hoe uiteindelijk wordt gehandeld als een betrokkene gegevensregistratie weigert is afhankelijk van de situatie. Uit het groepsgesprek komt naar voren dat soms wordt ingeschat dat nog een keer gesproken moet worden met de cliënt. In een ander geval komen ze na intern overleg tot de conclusie dat registratie wettelijk verplicht is. Een teamleider zegt: "*Er is iets aan de hand wanneer iemand dat niet wil. Eerst terug naar de persoon en uitleggen wat de gemeente doet aan het bieden van zorg. Wel letten op de zorgplicht die we als gemeente hebben. Dan doorpakken naar VT*[Veilig Thuis]*/GGD."* Een professional zegt: "*Hangt er vanaf: vrijwilligheid van de cliënt is niet hetzelfde voor de hulpverlener; die heeft soms dan toch* [te maken] *met verplichting van melding of registratie*."

6.4.3 Vast te leggen gegevens

Na het vragen van toestemming aan en het inlichten van de betrokkene worden de (bijzondere) persoonsgegevens ingevoerd in RIS. De hoeveelheid en aard van de gegevens verschilt per samenwerkingsketen. De respondenten van Samen DOEN lijken meer gegevens in te voeren in RIS dan Wijkzorg of OKT. Circa tweederde van de respondenten van Samen DOEN geeft aan dat ze zoveel mogelijk gegevens in RIS invullen die, eventueel later, gebruikt kunnen worden voor de hulpverlening. Voor Wijkzorg is dat een kwart van de respondenten. Dit zou een aanwijzing kunnen zijn dat in sommige gevallen de gegevensverzameling bovenmatig is.

Een derde van de respondenten voert de verkregen gegevens niet in omdat ze te privacygevoelig zouden zijn. Een paar respondenten heeft aangegeven dat zij zo handelen omdat zij twijfels hebben over wie de gegevens allemaal in kunnen zien. Ook twijfelen respondenten over het vastleggen van BSN-nummers. Sommige respondenten vragen zich – in lijn van de Wbp - af of dit wel noodzakelijk is. Gegeven de voorwaarden om een BSN te mogen verwerken lijkt deze kritische houding terecht (zie paragraaf 5.4.4).

Focusgroep Samen DOEN

De RIS-module biedt volgens de focusgroep ruim voldoende mogelijkheden om gegevens te registreren. Van deze mogelijkheid wordt gebruikgemaakt, omdat het registreren van zo veel mogelijk gegevens kan helpen om later op terug te vallen bij het verlenen van hulp. De helft van de medewerkers ervaart het invullen van de gegevens (enigszins) als een administratieve last. Zij zijn ook niet positief over de mate waarin het systeem ze ondersteunt bij het uitvoeren van taken. Voor een medewerker zijn de bevoegdheden niet helemaal duidelijk: *"Dacht dat het verwijderen van cliënten uit het RIS systeem verboden is. Omdat alle cliënten waar hulp is geweest of nog is recht hebben op het inzien van hun dossier ook nadat de hulp gestopt is."*

Andere manieren van gegevens vastleggen
De mate waarin de respondenten ook andere middelen, dan de RIS-module, gebruiken om gegevens vast te leggen, hangt sterk af van de samenwerkingsketen. Van de Samen DOEN-respondenten maakt circa een derde van de respondenten gebruik van andere manieren om gegevens vast te leggen. Bij de respondenten van OKT is dit percentage ongeveer 69%. Respondenten van Wijkzorg gebruiken zelfs voor 91% andere manieren van registreren. Deze hoge percentages worden grotendeels verklaard omdat de professionals vaak vanuit hun eigen organisatie verplicht zijn ook een intern registratiesysteem te gebruiken. Maar daarnaast worden ook andere middelen gebruikt om persoonsgegevens (tijdelijk) vast te leggen.

Focusgroep Samen DOEN
Het gaat hier vaak om de schriftelijke notities van de professional zelf. Soms registreren zij niet in RIS omdat ze de informatie te privacygevoelig vinden en enkele medewerkers zeggen dat ze meer informatie nodig hebben voor een goede hulpverlening (denk aan informatie over medicijngebruik of psychiatrische klachten). Soms is het maken van wat notities gemakkelijker omdat het handzamer is (zie tekstkader). Gegevens worden dan nadien vaak wel in RIS verwerkt en er wordt door sommige professionals benadrukt dat notities dan worden vernietigd of op een veilige plek worden bewaard. Een enkeling geeft hier aan mailtjes in de beveiligde mailbox te bewaren.

> *Ik maak aantekeningen in mijn schrift, in steekwoorden. Met als doel informatie niet te verliezen en ook met als doel om het vervolgens in RIS te kunnen zetten.*

Zelfredzaamheidsmatrix
De mate waarin de zelfredzaamheidsmatrix (ZRM) wordt gebruikt verschilt ook sterk tussen de respondenten van de verschillende RIS-modules. Ongeveer 90% van de respondenten van Samen DOEN en Wijkzorg meldt dat ze gebruik maken van de ZRM. Bij OKT is dit percentage maar 7%. Opmerkelijk, want over het gebruik van de ZRM in het privacyprotocol OKT is niets geregeld. Bij Samen DOEN geeft 28% van de respondenten aan zelf te mogen bepalen welke onderdelen van de ZRM ze mogen invullen (en 64% zegt dit niet te mogen). Bij Wijkzorg mag ongeveer de helft van de respondenten zelf bepalen welke onderdelen ze invullen. Dit is opvallend omdat bij de toelichting van de ZRM staat vermeld dat de professionals voor elk gezinslid, om de zes maanden en op elk van de domeinen een score in dient te vullen.[453]

Vervolgens is gevraagd in hoeverre de gegevens ook daadwerkelijk vastgelegd worden. Van de respondenten die gebruik maken van de ZRM zegt de helft dat er precies genoeg informatie over de cliënt wordt vastgelegd in de ZRM om hun taak te kunnen uitoefenen. Een kwart van de respondenten geeft aan dat er door de ZRM te weinig informatie over de cliënt wordt vastgelegd.

[453] Handleiding Registratieproces in RIS, Samen DOEN, 14-10-2013, p.6 en 8

De vraag kan worden gesteld of de professional goed zijn werk kan doen en of er in lijn met de Wbp niet bovenmatig wordt geregistreerd. Gegevens moeten immers toereikend zijn voor het doel van de gegevensverzameling. De instructie van de ZRM en de aanvullende instructies van leidinggevenden zouden hier meer duidelijkheid in kunnen verschaffen.

6.4.4 Conclusie

De verantwoordelijke heeft de plicht om de betrokkene tijdig te informeren over het doel van de gegevensverwerking (5.4). Over het algemeen wordt de norm uit de Wbp gehaald, maar niet altijd. De meeste professionals en ambtenaren geven aan vaak (22,9%) of altijd (56,2%) de betrokkene te informeren over het doel van de registratie. Hierbij moet opgemerkt worden dat er een kleine groep (19,3%) is die soms of nooit informeert. De focusgroep geeft aan dat zij verschillende motieven hebben om niet altijd te informeren, waaronder de reactie van de betrokkene of tijdgebrek.

Wat betreft toestemming bij het registreren van gegevens wordt vaker toestemming gevraagd dan volgens de privacyprotocollen nodig is. Wij vinden dit positief, omdat expliciete toestemming in tegenstelling tot impliciete of veronderstelde toestemming een goede waarborg is voor zorgvuldige gegevensverwerking (zie paragraaf 5.4.3).

De aanbeveling om bij de zelfredzaamheidsmatrix elk domein in te vullen, ook wanneer het niet strikt noodzakelijk is, is bovenmatig en niet conform de Wbp (zie paragraaf 5.4.4). Het lijkt de professionals niet duidelijk te zijn of, en zo ja, hoeveel ruimte ze hebben om hierin zelf afwegingen te maken.

6.5 Delen van gegevens

Voor de hulpverlening is het vaak noodzakelijk dat gegevens worden gedeeld met andere professionals en ambtenaren. Driekwart van de respondenten geeft aan gegevens te delen met andere professionals. Vooral respondenten van OKT (82%) doen dit. Dit percentage ligt lager bij respondenten van Wijkzorg (64%) en Samen DOEN (46%). Bijna tweederde van de respondenten van OKT vindt RIS ook een goed systeem om gegevens mee te delen. Dit aantal is ongeveer de helft minder bij respondenten van Samen DOEN en Wijkzorg. In deze paragraaf zetten we uiteen hoe professionals invulling geven aan het delen van gegevens en op welke wijze het delen wordt gecommuniceerd met de betrokkene.

6.5.1 Informeren betrokkene over delen van gegevens

De betrokkene zou altijd geïnformeerd moeten worden wanneer gegevens gedeeld worden met derden. Uit de enquête komt naar voren dat professionals en ambtenaren de betrokkene over het algemeen informeren voordat gegevens worden doorgegeven. Op het moment dat respondenten informatie van de betrokkene delen met derden,

informeren ze vaak (18%) tot altijd (75%) de betrokkene. De keren dat de betrokkene niet wordt geïnformeerd komt zelden voor, zo blijkt uit de enquête. Als dit wel gebeurt speelt de mate van urgentie en veiligheid een belangrijke rol: "*ik doe dit bijna altijd, maar er zijn situaties waarin dit niet mogelijk is bijvoorbeeld als de cliënt niet reageert en er omwille van veiligheid wel informatie gedeeld moet worden*". Ook wordt aangegeven dat het informeren van een betrokkene, net als het informeren over gegevensverwerking, verstorend kan werken: "*soms roept het alleen maar onrust op bij de klant omdat degene dit niet kan begrijpen waarom ik het doe*".

6.5.2 Toestemming betrokkene voor het delen van gegevens

Voor het vragen van toestemming voor het delen van gegevens kan gebruik worden gemaakt van een toestemmingsformulier. Zo heeft Samen DOEN een toestemmingsformulier dat de betrokkene dient te ondertekenen voordat gegevens worden opgevraagd bij derden. Het toestemmingsformulier geeft expliciet aan om welke (soorten) gegevens het gaat, wie de contactpersoon bij Samen DOEN is en met welke organisatie gegevens gedeeld worden.[454] Ook OKT maakt gebruik van een toestemmingsformulier. Het gaat hierbij om het opvragen van gegevens door de OKT-professionals bij een arts of specialist. Op het toestemmingsformulier dient specifiek aangegeven te worden welke gegevens met welk doel gedeeld worden. De betrokkene moet hier expliciet mee instemmen.[455] Bij Wijkzorg geeft de betrokkene toestemming voor het delen van gegevens op het moment dat hij het ondersteuningsplan tekent. Dit wordt aangegeven op het voorblad van het ondersteuningsplan.[456]

De meeste respondenten geven aan vaak (22%) tot altijd (74%) toestemming te vragen voor het delen van de gegevens. Wanneer geen toestemming wordt gevraagd worden daarvoor uiteenlopende redenen gegeven. Sommige respondenten geven als reden dat het gedeeld wordt met professionals binnen het team: "*Soms is de informatie binnen mijn team. Bijvoorbeeld een jeugdpsycholoog die actief gaat worden in het gezin en aan het dossier toegevoegd moet worden*." Of bijvoorbeeld bij mondeling overleg: "*Ik geef nooit een verslag door, of neem contact op met andere betrokken hulpverleners, zonder toestemming van een ouder. Maar mondeling overleg met een collega, mentor, zorg coördinator etc. gaat dan wel regelmatig zonder toestemming omdat deze afstemming belangrijk is*." Andere respondenten geven aan dat het situatieafhankelijk is. Vooral de veiligheid van het kind wordt als belangrijke reden om gegevens te delen zonder toestemming: "*Het om de kindveiligheid gaat en per direct informatie nodig is of doorgegeven moet worden vanwege het risico voor het kind. Naderhand zal cliënt altijd geïnformeerd worden van genomen actie*." In veel gevallen geeft de respondent aan dat ze naderhand de betrokkene informeren.

[454] Toestemmingsformulier uitwisselen gegevens Samen DOEN.

[455] Toestemmingsformulier opvragen zorggegevens OKT.

[456] Mail rekenkamer 15 december 2015.

6.5.3 Manieren om gegevens te delen

RIS is niet de enige manier waarop informatie wordt gedeeld. Informatie wordt veelal (ook) op andere wijzen gedeeld: via het werkoverleg, in gesprekken met andere professionals, via e-mail en telefoon. Ook worden gegevens gedeeld door middel van casuïstiek bespreking (zie paragrafen 4.4.2 en 5.3), verslaggeving of per post. Een minderheid zegt dat te doen via sms en Whatsapp (waarbij het dan bijvoorbeeld gaat om het sturen van een huisnummer dat een collega is vergeten). Redenen voor het delen van gegevens via andere systemen dan RIS zijn wisselend. De een zegt dat het sneller gaat dan via RIS, een ander geeft aan zo gemakkelijker informatie te kunnen delen met partijen die geen gebruik maken van RIS zoals de huisarts.

Focusgroep Samen DOEN

Binnen de teams zelf wordt ook regelmatig informatie gedeeld. Volgens de groep van Samen DOEN wordt de aanpak voor een specifieke betrokkene eerst binnen het eigen team besproken. Met het inbrengen van casussen wordt de beoogde aanpak getoetst of wordt er overlegd om gezamenlijk tot een goede oplossing te komen. Hoewel de casussen geanonimiseerd worden ingebracht herkennen professionals echter met regelmaat over welke gezinnen het gaat. Als het team er zelf niet uitkomt dan kunnen teamleiders en assistenten de casus of vraag vervolgens inbrengen in hun eigen overlegvormen – het *community practice overleg* – en de ingebrachte ideeën en oplossingen weer terugkoppelen naar het team.

Samen DOEN heeft een protocol beveiligd mailen. In dit protocol staat beschreven hoe je een Word- of pdf bestand beveiligd opslaat en is een stappenplan veilig versturen van vertrouwelijke informatie opgenomen.[457]

6.5.4 Conclusie

De professionals en ambtenaren informeren de betrokkene in 93% van de gevallen wanneer er gegevens gedeeld worden. Er wordt even vaak toestemming gevraagd voor het delen van gegevens. Wanneer de betrokkene niet wordt geïnformeerd, of er wordt geen toestemming gevraagd, wordt dit bijna altijd beargumenteerd vanuit de veiligheid of mate van urgentie van de specifieke situatie.

Er blijken veel verschillende manieren gebruikt te worden om gegevens te delen, wat een risico kan vormen voor de veiligheid van de persoonsgegevens. Gegevens worden bijvoorbeeld over de mail verzonden of worden telefonisch gedeeld. Dit kan een gevaar vormen wanneer persoonsgegevens via onbeschermde email verzonden worden of als wordt getelefoneerd in de openbare ruimte. Samen DOEN heeft een protocol beveiligd mailen, waar alle professionals zich aan dienen te houden, en gaat hier extra aandacht aan besteden in de leerlijn.

[457] Protocol Richtlijn voor beveiligd mailen met en tussen jeugdhulpverlener, Gemeente Amsterdam, 18 januari 2016

6.6 Rechten van betrokkenen

Betrokkenen hebben het recht om hun dossier in te zien, te veranderen of te verwijderen. In de volgende paragrafen gaan we nader in op het inzagerecht en het recht op correctie. [458]

Informeren van betrokkene over de rechten
De respondenten geven aan de betrokkenen niet altijd actief te informeren over de rechten. Bijna een kwart geeft aan dit (bijna) nooit te doen. In de toelichting wordt door sommige respondenten gemeld dat ze zelf niet volledig bekend zijn met de rechten van cliënten, of dat ze het alleen doen als de cliënt erom vraagt. Vanuit de focusgroep wordt aangegeven dat er nu geen document is waarin is vastgelegd wat precies aan de cliënt moet worden verteld.

6.6.1 Inzagerecht

Van het inzagerecht wordt maar weinig gebruik gemaakt. De helft van de respondenten geeft aan dat het verzoek van een betrokkene om gegevens in te zien nooit voorkomt en maar 2% dat dit met regelmaat voorkomt. Dit kan bij Samen DOEN worden verklaard doordat veel professionals het gezinsplan samen opstellen, waardoor de cliënt al een goed beeld heeft van de opgeslagen gegevens. Dit plan proberen professionals in eerste instantie fysiek mee te geven aan de cliënt.[459] Van de respondenten die weleens inzage hebben gegeven (N=181) meldt 80% een inzage altijd toe te staan.

De betrokkene heeft volgens het privacyprotocol recht op een afschrift (kopie) van de gegevens. Een derde van de respondenten geeft een print van het dossier mee aan de betrokkene. Een derde laat de betrokkene mee kijken in het systeem (RIS). Soms wordt een samenvatting van de belangrijkste informatie verstrekt.

Focusgroep Samen DOEN
Een aantal professionals geeft aan eerst te overleggen met de teamleider voordat ze inzage verstrekken. Een enkele respondent geeft aan dat ze de cliënt (bijna) nooit inzage geven. Hiervoor worden twee motieven genoemd. Het eerst motief is gescheiden ouders, waarbij geen informatie wordt verstrekt over de andere ouder. Het tweede motief is dat soms wordt vermoed dat de gegevens in een rechtszaak zullen worden gebruikt,hetgeen niet in lijn is met de Wbp.

De groep van Samen DOENers vindt RIS niet altijd een geschikt systeem om een betrokkene inzage te geven in zijn eigen dossier. Het systeem is op locatie vaak niet beschikbaar en de dossiers zijn gebaseerd op één huishouden wat betekent dat soms eerst voorwerk nodig is om de gegevens van andere gezinsleden af te schermen. Het plan dat wordt opgesteld in onderling overleg met het gezin wordt meestal in fysieke

[458] Zie ook artikel 22 van het privacyprotocol. Besloten is om *recht op verzet* en *recht op eigen verklaring* niet te beschrijven. We hebben hier niet naar gevraagd in de enquête, en wij schatten dat deze rechten niet frequent worden uitgeoefend in de praktijk.
[459] Interview 26-10-2015

vorm overhandigd, zodat het ook in het huishouden beschikbaar is. In RIS is het mogelijk een samenvatting te printen van het dossier, om aan het inzagerecht te voldoen.

6.6.2 Recht op correctie

Op het moment dat blijkt dat gegevens niet juist zijn vastgelegd heeft de betrokkene het recht zijn of haar gegevens te laten wijzigen of verwijderen. Een kwart van de respondenten heeft weleens het verzoek ontvangen gegevens te wijzigen of verwijderen. Van deze groep (N=106) wijzigt of verwijdert ongeveer 40% vaak tot altijd de gegevens als de betrokkene daarom vraagt. Daarentegen verwijdert 40% van de respondenten soms tot (bijna) nooit gegevens. De respondenten geven in hun toelichtingen aan dat het wijzigen of verwijderen van gegevens van de context afhangt. Ook melden ze dat ze bij het niet accepteren van de correctie een aantekening in het dossier maken.

Focusgroep Samen DOEN

De meerderheid van de professionals zegt niet te weten of het makkelijk of moeilijk is voor betrokkenen om een verzoek tot correctie in te dienen. Zij zeggen ook dat het (bijna) nooit voorkomt dat betrokkenen dit verzoeken. Als het wel gebeurt, lijkt het niet moeilijk te zijn het verzoek in RIS door te voeren. Uit de gegeven toelichtingen ontstaat een beeld dat professionals in de praktijk pragmatisch met 'verzoeken' omgaan: betrokkenen komen in de praktijk wel eens met vragen of opmerkingen. Deze worden wellicht niet als 'formeel' verzoek beschouwd en professionals reageren daar verschillend op. Een van de medewerkers zegt: *"Ik leg uit waarom* [ik gegevens niet wijzig] *en benoem concreet waar ik vind dat het niet gewijzigd of verwijderd kan worden en ben transparant hierin naar de cliënt toe."* Een andere oplossing is: *"Ik formuleer dat de cliënt het met de gegevens niet eens is."*

6.6.3 Conclusie

De betrokkenen hebben het recht gegevens in te zien en als gegevens onjuist zijn te laten wijzigen of vernietigen. Volgens de respondenten wordt van deze rechten nauwelijks gebruik gemaakt. Er is onder professionals veel onduidelijkheid over de manier waarop een verzoek behoorlijk dient te worden afgehandeld. De professionals worden hierover onvoldoende geschoold in trainingen met het gevolg dat de betrokkene onvoldoende wordt geïnformeerd over zijn rechten. Het systeem RIS is volgens de professionals ongeschikt voor het geven van inzage in gegevens.

6.7 Conclusie

In dit hoofdstuk hebben we gekeken hoe het proces van gegevensverwerking rondom de betrokkene verloopt en of dit in lijn is met de Wbp en aanvullende regelgeving. We hebben dit gedaan door te kijken naar de kennis van privacyregelgeving, de voorlichting aan de betrokkene via de website, folders en het privacyprotocol, registreren van gegevens, delen van gegevens en de rechten van de betrokkene.

Op een aantal punten zien we dat de normen in voldoende mate uitwerking krijgen in de praktijk. Daarbij worden de normen van de Wbp en de privacyprotocollen op het gebied van het informeren van en toestemming vragen aan de betrokkene bij zowel registratie als deling van gegevens in voldoende mate nageleefd. Op het moment dat de betrokkene om inzage vraagt geeft circa 80% van professionals en ambtenaren aan inzage te geven. Ook informeert ongeveer 80% van de ondervraagden vaak tot altijd wanneer ze persoonsgegevens van de betrokkene registreren. Toch zien we dat 20% dit soms tot nooit doet. In sommige gevallen zouden we mogen verwachten dat alle professionals en ambtenaren zich aan de norm houden. Op een aantal punten blijkt dat de privacyregels niet voldoende worden nageleefd.

Allereerst zien we dat professionals en ambtenaren regelmatig meer gegevens verwerken dan nodig is. Persoonsgegevens mogen alleen verwerkt worden wanneer het noodzakelijk is voor een goede hulpverlening aan de betrokkene (zie paragraaf 5.7). Uit de enquête blijkt dat tweederde van de Samen DOENers aangeeft zoveel mogelijk gegevens op te slaan die, eventueel later, gebruikt kunnen worden voor de hulpverlening. Daarnaast wordt gebruikers van RIS aanbevolen alle gegevens in de zelfredzaamheidmatrix (ZRM) in te vullen (zie paragraaf 5.7). Uit de enquête blijkt dat 64% van de Samen DOENers niet zelf mogen bepalen welke leefdomeinen zij invullen. Dit is te verklaren doordat de ZRM ook wordt gebruikt als meetinstrument om de effectiviteit van het programma te kunnen bepalen (zie paragraaf 5.4.4). Beide situaties vergroten het risico op bovenmatige gegevensverwerking.

Ten tweede constateren we dat de betrokkene onvoldoende wordt voorgelicht over zijn rechten en verzoeken tot wijziging of verwijdering van gegevens. Deze verzoeken worden niet altijd gehonoreerd. Een kwart van de professionals en ambtenaren geeft aan (bijna) nooit de betrokkene te informeren over zijn rechten. Tegelijk constateren we dat 90% van professionals en ambtenaren aangeven (bijna) nooit een verzoek tot inzage in hun dossier te hebben ontvangen. Op het moment dat betrokkene een verzoek tot wijziging of verwijdering van gegevens doet, geeft meer dan 40% aan soms of nooit gegevens te wijzigen of te verwijderen.

Ten derde constateren we dat 70% van de professionals en ambtenaren aangeven andere manieren te gebruiken om gegevens vast te leggen dan in het RIS-systeem. Dit is deels verklaarbaar doordat professionals verplicht zijn andere systemen te gebruiken dan het RIS-systeem. Echter gaat hier ook vaak om de schriftelijke notities van de hulpverlener zelf. Het college kan er dan niet op toezien dat gegevens veilig en

zorgvuldig worden gearchiveerd. Positief is dat Samen DOEN dit onderkent en hier meer aandacht aan gaat besteden in de leerlijn.

Tot slot zien we rondom voorlichting dat er meerdere kanalen zijn om de betrokkene te informeren, maar dat professionals en ambtenaren dit niet altijd actief doen. De belangenafweging die een professional of ambtenaar maakt wordt verder uitgewerkt in het volgende hoofdstuk.

7 De balans tussen privacy en gegevensverwerking in de praktijk

Bij het maken van de afweging welke gegevens verwerkt dienen te worden zou zoveel mogelijk de betrokkene en zijn hulpvraag centraal moeten staan. Dit zonder dat daarbij de privacybescherming en de regelgeving over het verwerken van persoonsgegevens terzijde wordt gesteld of wordt veronachtzaamd.[460]

Om deze belangen goed te kunnen wegen moeten professionals en ambtenaren het vermogen hebben om precies te kunnen bepalen welke gegevens noodzakelijk zijn om de hulp te verlenen die gevraagd wordt. Als deze afweging niet goed kan worden gemaakt dan kan de situatie ontstaan dat er standaard gegevens worden gevraagd en verwerkt die veel verder gaan dan voor de hulpvraag van de betrokkene noodzakelijk is. De gegevensverwerking is dan niet passend voor de hulpverlening. Anderzijds kan een nadruk op regels ter bescherming van privacy de professional of ambtenaar onzeker of kopschuw maken – bijvoorbeeld in het geval van delen van gegevens – wat ook niet bijdraagt aan een goede dienstverlening waarbij de betrokkene de ondersteuning ontvangt die nodig is.[461]

In dit hoofdstuk staat de vraag centraal:

Wat is de balans tussen privacy en gegevensverwerking in de praktijk?

Het maken van een dergelijke belangenafweging is eenvoudiger wanneer de randvoorwaarden op orde zijn. In paragraaf 7.1 beantwoorden wij de vraag of volgens de professionals en ambtenaren de randvoorwaarden voldoende zijn ingevuld om een afweging te kunnen maken tussen het belang van een adequate gegevensverwerking en een respectvolle omgang met privacy.

Het feit dat de gegevensverwerking moet passen bij de hulpvraag van betrokkene en zijn of haar recht op regie, betekent niet dat er geen situaties kunnen ontstaan waarin gegevensdeling zonder toestemming van de betrokkene noodzakelijk wordt geacht door de professional of ambtenaar. In paragraaf 7.2 hebben wij een aantal van deze situaties aan hen voorgelegd om na te kunnen gaan hoe dit zoeken naar balans in de praktijk werkt.

7.1 Randvoorwaarden voor het kunnen zoeken naar balans

In deze paragraaf gaan we in op de randvoorwaarden die de organisatie kan creëren om de werkzaamheden adequaat te kunnen uitvoeren met respect voor de privacy van de betrokkene. Deze randvoorwaarden kunnen enerzijds te maken hebben met het waarborgen van privacy en anderzijds met het efficiënt en effectief uitvoeren van

[460] Minister van Binnenlandse Zaken en Koninkrijksrelaties, Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Aandachtspunten, risico's en suggesties voor gegevensverwerking bij de uitvoering van de gemeentelijke taken en werkzaamheden in een gedecentraliseerd sociaal domein, 7 november 2014, p. 4

[461] Idem.

de werkzaamheden. We beschrijven vier van deze randvoorwaarden zoals die uit de enquête en de focusgroep[462] naar voren zijn gekomen. Deze randvoorwaarden hebben te maken met de invloed van de privacyregelgeving op de werkzaamheden, het belang dat de organisatie aan privacy hecht, de ondersteuning (functionaliteit en autorisatie) die RIS biedt aan de werkzaamheden en de ervaringen met dossiervorming bij gegevensverwerking.

7.1.1 Invloed privacyregelgeving op de werkzaamheden

Bij de eerste randvoorwaarde gaat het over de invloed van de privacyregelgeving op de werkzaamheden. Professionals en ambtenaren moeten de privacyregelgeving niet als belemmerend gaan ervaren bij hun werkzaamheden. Dat kan namelijk tot gevolg hebben dat in de belangenafweging privacy te weinig aandacht krijgt of het werk niet meer efficiënt verloopt

We beschouwen dit in orde als minimaal tweederde van de ondervraagden de privacyregelgeving niet als belemmerend ervaart. Aan deze criteria wordt niet helemaal voldaan. Uit de enquête blijkt dat 42% van de ondervraagden de regelgeving niet als belemmerend ervaart en 17% als wel belemmerd. De overige professionals en ambtenaren weten niet wat ze moeten antwoorden of hebben een neutrale mening. Deze onzekerheid zien we ook terug in de reacties op de ”Ik moet bij de hulpverlening te veel rekening houden met de privacy van cliënten”. In dit geval geeft een derde aan niet te weten wat ze moeten antwoorden of heeft een neutrale mening. Ongeveer de helft ondervraagden is van mening dat ze niet te veel rekening hoeven te houden met de privacy van cliënten. Ongeveer 16% vindt wèl dat ze te veel rekening moeten houden met de privacy van cliënten.

Uit het bovenstaande blijkt dat voor een deel van de professionals en ambtenaren de privacyregelgeving een efficiënte en effectieve taakuitvoering in de weg staat. Uit verdere analyse blijkt dat dit gevoel van belemmering door de regels samenhangt met de mate waarin ambtenaren en hulpverleners de privacyregelgeving complex vinden. Een vergelijkbaar effect zien we terug bij de stelling dat er te veel rekening moet worden gehouden met de privacy van de cliënten. Er zou dus iets gedaan kunnen worden aan het verbeteren van deze randvoorwaarde door de regels uit te leggen en begrijpelijker te communiceren.

[462] De focusgroep bestaat uit respondenten van Samen DOEN en Samen DOENers die aan het groepsgesprek hebben deelgenomen. Zie ook inleiding hoofdstuk 6.

7.2 Belang dat organisatie aan privacy hecht

De volgende randvoorwaarde die we bespreken is de mate waarin de organisatie[463] belang hecht aan privacy. Wanneer in woord en daad het belang van privacy wordt uitgedragen binnen de organisatie verwachten we dat dit van invloed zal zijn op de wijze waarop professionals en ambtenaren belangen afwegen. De organisatie kan dat uitdragen door correct met cliëntgegevens om te gaan en hulpverleners kennis van privacy bij te brengen. Daarnaast kan de organisatie ook medewerkers scholen en actief informeren over privacyregels of privacyvraagstukken

Aandacht organisatie
We denken dat de organisatie voldoende aandacht aan privacy geeft als ongeveer minimaal tweederde van de professionals en ambtenaren dit ook zo ervaart. Uit de enquête blijkt dat circa 70% van de professionals en ambtenaren van mening is dat hun organisatie zorgvuldig omgaat met privacygevoelige gegevens. Tweederde van de ondervraagden onderschrijft ook de stelling dat de werkomgeving genoeg aandacht heeft voor privacy en ook ongeveer tweederde geeft aan dat ze het gevoel hebben dat binnen de organisatie alleen gegevens worden verstrekt aan anderen als dat volgens de regels mag. De reacties op de stellingen hangen ook onderling samen.[464]

Uit de reacties die professionals en ambtenaren in de enquête geven, blijkt ook dat er in de organisatie aandacht wordt besteed aan de privacyregelgeving. Dat wil echter niet zeggen dat ze altijd goed op de hoogte zijn. Bij bijvoorbeeld het verstrekken van informatie over de rechten van de betrokkene stellen meerdere professionals en ambtenaren dat ze onbekend zijn met die rechten (zie ook paragraaf 6.5).

Scholingsmogelijkheden
Voor de ontwikkeling van kennis over privacyregels is het belangrijk dat de organisatie scholingsmogelijkheden aanbiedt aan professionals en ambtenaren. Wij achten de scholingsmogelijkheden voldoende op niveau als minimaal ongeveer tweederde van de professionals en ambtenaren dit ook zo ervaart. Dat blijkt niet het geval te zijn; ze zijn kritisch. Het verwerven en onderhouden van kennis via scholing blijkt lastig. Een kwart van de respondenten meldt niet voldoende scholingsmogelijkheden te krijgen om de kennis over de omgang met privacygevoelige gegevens te vergroten. Wat opvalt uit de reacties is dat sommigen aangeven dat ze wel scholing hebben gehad maar dat de scholing om verschillende redenen niet breed is uitgerold. Sommigen vragen zich af of collega's wel de kennis hebben die nodig is.

De kritische houding van de professionals en ambtenaren is opvallend omdat ze wel positief zijn over hun kennis van de privacyregelgeving (zie paragraaf 6.2). Mogelijk komt dit doordat voor een deel van de professionals en ambtenaren het medische

[463] Onder organisatie verstaan we de gemeente en de voor de respondent relevante zorg- en welzijnsinstellingen.
[464] Samenhang tussen "zorgvuldige omgang" en "voldoende aandacht: correlatiecoëfficiënt; 0,63, significantielevel: p<0,01. Samenhang tussen "zorgvuldige omgang" en "alleen als het mag": correlatiecoëfficiënt: 0,53, significantielevel: p<0,01.Correlatiecoëfficiënt: 0,63; significantielevel: p<0,01.

beroepsgeheim van toepassing is en zij vanuit hun beroepsopleiding hiervoor uitgebreid zijn geschoold. Privacyregels gaan echter verder dan het medische beroepsgeheim. Bovendien hebben niet alle professionals en ambtenaren een beroepsgeheim en van de daarbij behorende scholing genoten. De verantwoordelijkheid voor het vergaren van kennis ligt natuurlijk ook bij persoon zelf, maar de organisatie draagt de verantwoordelijkheid om scholingsmogelijkheden te faciliteren.

Volgens de focusgroep zou een oplossing zijn om het privacyprotocol als standaard onderdeel van het inwerkprogramma voor nieuwe medewerkers op te nemen. Een deelnemer van het groepsgesprek geeft aan een presentatie over privacyregelgeving te hebben bijgewoond en is daar enthousiast over. Vanuit de groep wordt aangegeven dat de gemeente het voornemen heeft om een aparte leermodule te laten ontwikkelen. Bovendien zal de nieuwe versie van het privacyprotocol (oktober 2015) aan ieder team worden gepresenteerd. De verwachting van de focusgroep is dat daarmee het thema privacy goed onder de aandacht zal worden gebracht.

Daarnaast stelt de focusgroep dat de scholingsmogelijkheden een leerlijn moeten bevatten die richting geeft bij verzoeken van de cliënt om de eigen gegevens te wijzigen of verwijderen en als een cliënt geen toestemming geeft voor het registreren van persoonlijke gegevens.

Actief informeren
De mate waarop professionals en ambtenaren op de hoogte worden gehouden door hun organisatie over gewijzigde privacyregels of privacyvraagstukken wordt als te minimaal ervaren. Wederom gaan we ervan uit dat als minimaal tweederde van de ondervraagden ervaart dat ze goed worden geïnformeerd, de organisatie op dat punt voldoende actief is. Uit de enquête blijkt echter dat slechts 29% vindt dat de organisatie hen actief informeert. 39% twijfelt en is van mening dat ze een beetje op de hoogte worden gehouden. Van de rest van de professionals en ambtenaren is 26% kritisch en 7% geeft aan niet te weten wat ze moeten. Het is lastig om alles tot in detail over de privacyregelgeving paraat te hebben als er veel verandert in de wet- en regelgeving én in het RIS-systeem zelf.

7.2.1 Ondersteuning RIS
De derde randvoorwaarde gaat over het registratiesysteem RIS. Hierbij gaan we in op de functionaliteit van RIS met de vraag of die ondersteunend is aan het kunnen maken van een goede belangenafweging. Daarnaast behandelen we de vraag of de autorisaties in RIS goed geregeld zijn.

Functionaliteit van RIS
De functionaliteit van het geautomatiseerde systeem is een belangrijke randvoorwaarde voor het efficiënt en effectief uitvoeren van de taken en het respecteren van de privacy. Bij de functionaliteit van RIS draait het om de vraag in welke mate het systeem ondersteunend is aan of juist belemmerend werkt bij het uitvoeren van taken. Willen we het gevoel hebben de functionaliteit van RIS op orde is, dan mogen we ervan uitgaan dat zeker tweederde van de professionals en ambtenaren dit ook vindt.

Uit de enquête blijk dat dit criterium niet wordt gehaald. Slechts 22% van de respondenten vindt RIS een overzichtelijk en gebruiksvriendelijk systeem. Ongeveer een derde van de respondenten reageert neutraal op de vraag en circa 43% is uitgesproken negatief. Ook vindt bijna 50% van de respondenten RIS niet aansluiten op de dagelijkse werkpraktijk en circa 45% dat in RIS gegevens niet snel en eenvoudig te raadplegen zijn. Een respondent geeft de volgende toelichting op dit onderwerp: "*Informatie is verscholen. Alles is met doorklikken. Zowel persoonsgegevens, als contacten, als plan van aanpak. Het is traag en werkt in bepaalde omgevingen erg moeilijk. Het is een ontransparant systeem. (…) Ik krijg veel klachten. Ik heb een tijd in de RIS werkgroep gezeten en we probeerden het beter te maken. Echter is de template van het systeem beperkt en kunnen er relatief gezien kleine veranderingen worden doorgezet maar het is meer symptoombestrijding.*"

Onder de respondenten leeft dus een behoorlijk negatief beeld ten aanzien van de functionaliteit. In de focusgroep met Samen DOENers is gemeld dat de functionaliteit wel veel aandacht krijgt vanuit het programmateam. Samen wordt er gezocht naar passende verbeteringen.

Het cluster sociaal heeft ter toelichting aangegeven dat zij dit beeld herkent. Onduidelijk werkprocessen en werkprocessen die vaak veranderen, maken het werken met het registratiesysteem RIS lastig. Ook wordt aangegeven dat de organisaties van OKT en Wijkzorg nog in ontwikkeling zijn[465] Aan de ontwikkeling van functionaliteit wordt gewerkt. Bij OKT zijn er veel technische aanpassingen geweest om de gebruikerservaring te verbeteren en wordt gezocht naar een goede balans tussen gegevenswerking en privacy van burgers.[466] Ook bij Wijkzorg zijn klachten binnen gekomen over de functionaliteit. Deze zijn opgepakt door IV sociaal en een extern bureau heeft hier onderzoek naar gedaan.[467] Bevindingen worden geanalyseerd, geprioriteerd en doorgevoerd.[468]

Autorisatie
Een andere belangrijke randvoorwaarde is dat de autorisatie rondom persoonsgegevens in orde is. Dit betekent dat alleen bevoegde professionals en ambtenaren toegang hebben tot het dossier. We mogen ervan uitgaan dat dit op orde is. Het criterium dat daarbij past is dat bij voorkeur 100% van de professionals en ambtenaren dit zo ervaart. De ondervraagden hebben hier echter hun twijfels over. Uit de enquête blijkt dat 37% van mening is dat in RIS alle gegevens voldoende veilig beschermd zijn. Daarnaast heeft circa de helft twijfels of alleen de professionals en

[465] Stedelijk directeur sociaal, feitelijk wederhoor, 17-2-2016.
[466] In het kader van het feitelijk wederhoor is de Rekenkamer een Excel-bestand toegestuurd met de titel "RIS OKT techniekissues". Hierin is een actielijst opgenomen om technische issues op te nemen, in actie te zetten en door te voeren.
[467] Inview, Adviesrapport RIS Wijkzorg 2nd opninion. Een perspectief voor de korte termijn, 27 november 2015.
[468] Stedelijk directeur sociaal, feitelijk wederhoor, 17-2-2016

ambtenaren die dat mogen toegang hebben tot de gegevens van betrokkenen. Deze percentages liggen daarmee fors onder ons criterium.

In de toelichtingen die de professionals en ambtenaren geven, wordt aangegeven dat de ze geen zicht hebben wie gegevens van betrokkenen kunnen inzien. Professionals en ambtenaren die wel weten wie gegevens kunnen inzien zijn ook niet tevreden: "*RIS beschermt de privacy onvoldoende. Een OKA [Ouder- en Kindadviseur] kan als meekijker van een Jeugdpsycholoog overal in. Dat zou niet moeten mogen. Onze dossier-voering als BIG-geregistreerde GZ-psycholoog mag niet inzichtelijk zijn voor een OKA. Nu moet op vertrouwen gewerkt worden (dat een OKA de contacten niet opent), maar dat is niet zoals het hoort.*" Het bovenstaande laat zien dat er meer duidelijkheid geschapen moet worden hoe gegevens in RIS verwerkt worden en er meer transparantie moet komen over wie bevoegd is om de gegevens in te kunnen zien. Des te meer omdat de autorisaties redelijk op orde zijn (zie paragraaf 4.3.2). Door de onduidelijkheid over de transparantie in de autorisaties geven sommigen aan dat ze daarom minder gegevens invoeren.

Ook het niveau waarop de informatie mag worden ingezien vereist transparantie. Hierbij is van belang het verschil tussen 'dat'-informatie en 'wat'-informatie. Een oud RIS-gebruiker uit de enquête zegt hier het volgende over: *Een belangrijk onderscheid dat in de vraagstelling mist is het verschil tussen het uitwisselen van 'DAT informatie'(zonder dossierinhoud) en 'WAT informatie'tussen zorgpartners. Zonder privacy te schaden is veelal goed verdedigbaar dat zorgpartijen snel coördineren met andere betrokken professionals, binnen een gedefinieerd convenant. Daarna kan worden bek[ek]en of [het]uitwisselen van inhoudelijke informatie in het belang van de cliënt is, waarbij de basis is dat er toestemming nodig is, tenzij kan worden verantwoord dat de belangen of de veiligheid van de cliënt en soms de omgeving prioriteit krijgen boven deze expliciete toestemming*."

7.2.2 Dossiervorming

De laatste randvoorwaarde die we bespreken gaat over dossiervorming. Professionals en ambtenaren moeten voor een goede uitvoering van hun taak de juiste hoeveelheid gegevens kunnen invoeren en ze moeten het vertrouwen hebben dat gegevens die anderen hebben ingevoerd betrouwbaar zijn.

Op niet passende wijze gegevens invoeren

Het is niet de bedoeling dat er te veel of juist te weinig gegevens worden verzameld en worden vastgelegd. Dit zou ervoor kunnen zorgen dat de gegevensverzameling niet ter zake dienend, bovenmatig of juist onvolledig is, gelet op de doeleinden waarvoor zij verzameld en verwerkt wordt. De organisatie moet er voor zorgen dat het belang hiervan wordt onderstreept. Wij denken dat de organisatie dat in voldoende mate doet als ten minste tweederde van de professionals en ambtenaren ervaren dat ze niet te veel gegevens moeten uitvragen en registreren.

Aan het criterium wordt niet voldaan. Slechts een derde van de professionals en ambtenaren geeft echter aan dat ze in RIS meer gegevens moeten invullen voor het

uitvoeren van hun taak en voor een goede hulpverlening. Dit zou een aanwijzing kunnen zijn dat in sommige gevallen de gegevensverzameling bovenmatig is.

Gegevens betrouwbaar
In het belang van het waarborgen van de privacyregelgeving en een effectieve en efficiënte hulpverlening is het van belang dat gegevens betrouwbaar zijn. Het gaat niet alleen om wát wordt geregistreerd, maar ook om hoe men dat formuleert. Het vastleggen van een specifieke aanpak, inclusief de argumentatie hiervoor, in een dossier kan lastig zijn, zeker als een hulpverlener verwacht dat een cliënt om inzage zal vragen. Een professional en ambtenaar mag ervan uitgaan dat de gegevens die geregistreerd zijn volledig in orde zijn. Een passend criterium hierbij is 100%.

In de reactie van een aanzienlijk deel van de professionals en ambtenaren schuilt echter een bepaalde mate van onzekerheid. Een kwart geeft aan niet te weten wat ze moeten antwoorden en circa 40% reageert neutraal. Dat kan te maken hebben met het feit dat het voor hulpverleners lastig (snel) te controleren of de gegevens die zijn ingevoerd betrouwbaar zijn, maar het kan ook gezien worden als een teken van wantrouwen. Hoe het ook zij: in beide gevallen is er sprake van weinig vertrouwen in de dossiervorming. Slechts 20% van de professionals en ambtenaren gaf aan te weten dat de gegevens die door anderen zijn ingevuld betrouwbaar zijn.

7.2.3 Conclusie
Wanneer randvoorwaarden op orde zijn is het voor de professionals en ambtenaren makkelijker om een belangenafweging te maken tussen een adequate gegevens-verwerking en respectvolle omgang met privacy. De professionals en ambtenaren zijn over het algemeen positief over de organisatorische randvoorwaarden. Dit blijkt uit het gegeven dat:
- circa 70% vindt dat de *organisatie zorgvuldig* met privacygevoelige informatie omgaat;
- tweederde van mening is dat de *werkomgeving voldoende aandacht* besteed aan privacy.

Over de andere randvoorwaarden zijn de professionals en ambtenaren kritisch. Dit blijkt uit de uitkomst dat:
- slechts 42% de *privacyregelgeving* niet als belemmerend ervaart;
- maar een derde van mening is dat de *scholingsmogelijkheden* op orde zijn;
- maar circa een kwart van de professionals en ambtenaren RIS gebruiksvriendelijk en overzichtelijk (*functionaliteit*) vindt en slechts 37% stelt dat in RIS alle gegevens voldoende veilig zijn beschermd en de helft heeft twijfels of alleen de professionals die dat mogen toegang hebben tot de gegevens van betrokkenen (*autorisaties*);
- ongeveer een derde vindt dat ze in RIS te veel gegevens moeten invoeren (*bovenmatige gegevensverzameling)* en slechts 20% van de respondenten zeker is dat de gegevens die door anderen zijn ingevuld *betrouwbaar* zijn.

Gegeven het aantal kanttekeningen die de professionals en ambtenaren ervaren, vinden wij de randvoorwaarden op onvoldoende niveau om ondersteunend te zijn aan de belangenafweging.

7.3 Belangenafweging in praktijksituaties

In de vorige paragraaf hebben we gezien dat professionals en ambtenaren kanttekeningen hebben geplaatst bij het niveau van de randvoorwaarden die van belang zijn voor een belangenafweging tussen een adequate gegevensverwerking en respectvolle omgang met privacy. Dit bemoeilijkt de belangenafweging. In deze paragraaf bespreken we een aantal praktijksituaties die aan de professionals en ambtenaren zijn voorgelegd om na te gaan waar de belangenafweging in resulteert.

De belangafweging bij het delen van gegevens en respecteren van de privacy is geregeld een grijs gebied. We zien dit ook goed terug bij volgende stelling: *Als de hulpverlening er mee gediend is moet niet zo moeilijk worden gedaan over het verstrekken van gegevens van cliënten [betrokkenen] aan andere betrokkenen*. Met deze stelling is slechts ongeveer 40% van de professionals en ambtenaren het (helemaal) mee oneens. Zij geven aan zich te allen tijde aan de privacyregelgeving te houden en uitsluitend gegevens te delen in samenspraak met de cliënt. Een kwart is het daarentegen wel eens met de stelling. Zij vinden de hulpverlening voorop staan. De rest reageert neutraal of weet niet wat ze moeten antwoorden op de stelling. De antwoorden van de professionals en ambtenaren doen vermoeden dat in dit grijze gebied een werkwijze wordt gehanteerd waarin positief geformuleerd 'maatwerk' voorop staat.

De uiteenlopende uitkomsten van belangenafweging in de hierboven geschetste stelling zien we ook terug in 12 praktijksituaties (tabel 7.1 en 7.2) die aan de professionals en ambtenaren zijn voorgelegd. We signaleren twee soorten uitkomsten. Soms is er sprake van grote eensgezindheid. In deze situaties constateren we een consistente wijze van werken. Dit noemen we praktijknormen. Deze normen worden niet afgedwongen maar wel door een grote groep gehandhaafd. Het is soms ook zo dat professionals en ambtenaren onderling sterk verdeeld lijken. De praktijknorm is dan minder goed zichtbaar of er is geen praktijknorm.

De hieronder beschreven praktijksituaties zijn van extra relevantie omdat vaak 'escalatie' van de situatie centraal staat. Dit betekent dat de professional of ambtenaar in de belangenafweging tot de conclusie komt dat het niet ondernemen van verdere actie een situatie oplevert waarin de gezondheid of de veiligheid van betrokkene en/of zijn omgeving niet meer gegarandeerd is. Tegelijk kan het delen van gegevens een (zware) inbreuk zijn op de privacy van de betrokkene.

7.3.1 Eensgezindheid

We spreken van een praktijknorm als uit de enquête blijkt dat ongeveer tweederde van de professionals en ambtenaren eensgezind is over de vraag of gegevens wel of

niet gedeeld mogen worden. In tabel 7.1 is een overzicht weergegeven van praktijksituaties waarover professionals en ambtenaren eensgezind zijn.

Tabel 7.1 -Situaties waarin eensgezindheid is over het delen van gegevens

	Mag wel	Mag niet	Hangt er van af	Weet niet
Veiligheid van kinderen **(+)** [469]	81,0 %	1,9%	15,1%	1,9%
Efficiënte informatie uitwisseling **(+)**[470]	7,2%	56,4%	29,1%	7,4%
Betere dienstverlening aan de cliënt	6,6%	58,7%	30,4%	4,3%
Cliënten die Nederlandse taal niet machtig zijn	3,5%	65,5%	26,4%	4,7%

Toelichting: + Wettelijke grondslag

Wel delen

Uit de enquête blijkt dat als de veiligheid van het kind in het geding is, 81% van de professionals en ambtenaren van mening is dat gegevens wel gedeeld mogen worden. Dit is duidelijk een praktijknorm. Ook in de focusgroep met Samen DOENers werd de veiligheid van het kind als belangrijkste reden gezien om gegevens te delen met derden. Dit komt ook meermaals terug in de toelichtingen. Een voorbeeld: "*Binnen het OKT is voor mij de veiligheid van het kind de belangrijkste reden om privacyregels eventueel te schenden*.[..]" De focusgroep ziet echter ook een valkuil in het frequent kwalificeren van kindveiligheid als reden om soepeler om te gaan met de privacyregelgeving. Hierin ligt namelijk het risico verscholen dat professionals en ambtenaren situaties van ernstig gevaar steeds wat meer gaan oprekken: *"Er wordt nogal eens te snel gegrepen naar het instrument kindveiligheid omdat in het kader daarvan alles is geoorloofd."*

Niet delen

In het geval dat betrokkenen de Nederlandse taal niet machtig zijn, is ongeveer tweederde van de professionals en ambtenaren van mening dat gegevens niet gedeeld mogen worden. In de buurt van het criterium vallen de situaties dat het delen van gegevens voor een efficiëntere informatie-uitwisseling zorgt en een betere dienstverlening aan de cliënt oplevert. Ook de focusgroep is eensluidend van oordeel dat het delen van gegevens zonder toestemming van de betrokkene niet mag om de dienstverlening te verbeteren of om het uitwisselen van informatie efficiënter te laten verlopen. Vanuit het programmateam komt de opmerking dat het efficiënt kan zijn om autorisaties per team te geven, zodat collega's dan inzicht kunnen hebben in elkaars dossiers. Dit kan handig zijn in geval van (langdurige) ziekte. Teamleden hebben hier echter geen opmerkingen over gemaakt.

[469] Art. 7.3.2 lid 3 en art 7.3.11 lid 4 Jeugdwet.

[470] Voor zover het nodig is voor beleidsvorming;. Art. 7.4.1 Jeugdwet.

7.3.2 Verdeeldheid

In tabel 7.2 is een overzicht weergegeven van praktijksituaties waarover professionals en ambtenaren van mening verschillen. We onderscheiden daarbij drie soorten situaties : praktijksituaties waarbij vaak wordt gezegd 'hangt er van af', praktijk-situaties waarbij zowel redelijk vaak het antwoord 'mag wel' als het antwoord 'mag niet' wordt gegeven en tot slot praktijksituaties waarin velen het 'niet weten'.

Tabel 7.2-Situaties waarin verdeeldheid is over het delen van gegevens

	Mag wel	Mag niet	Hangt er van af	Weet niet
Zorgmijdend gedrag **(+)**[471]	20,2%	18,4%	58,3%	3,1%
Vermoeden van fraude	18,2%	28,5%	41,7%	11,6%
Vermoeden van criminaliteit, anders dan fraude	24,8%	18,2%	48,3%	8,7%
Gezondheidsrisico's voor de cliënt **(+)**[472]	23,4%	20,0%	51,6%	5,0%
Overlast voor de omgeving van de cliënt	10,9%	36,4%	46,3%	6,4%
Veiligheid van cliënt (geen kind)	39,0%	10,9%	45,7%	4,5%
Cliënten met een verstandelijke/geestelijke beperking	6,4%	36,4%	50,2%	7,0%
Een informeel signaal dat iemand mogelijk hulp nodig heeft **(+)**[473]	10,1%	44,0%	41,9%	4,1%

Toelichting: + Wettelijke grondslag

Hangt er van af, praktijknorm?
In dit geval is men het eens over het feit dat de beslissing sterk afhangt van de situatie. Dat kan een praktijknorm worden genoemd. Situaties waarbij ongeveer de helft of meer van de ondervraagden dit vindt, zijn: in het geval van zorgmijdend gedrag, gezondheidsrisico's voor de betrokkene en als de betrokkene een verstandelijke of geestelijke beperking heeft.

Het eens zijn over het feit dat de beslissing afhankelijk is van de context, wil niet zeggen dat men bij die afweging altijd dezelfde richting in zal slaan. In de toelichting wordt vaak ingegaan op deze 'hangt-er-van-af'-situatie. Daaruit blijkt wel dat men vindt dat je toch niet goed kan handelen zonder een zekere professionele vrijheid. Een professional zegt: "*je moet steeds goed het belang voor de cliënt afwegen. Indien je toch informatie hebt verstrekt moet je dat achteraf altijd melden en toelichten aan de cliënt*." Dat hierin een bepaalde mate van professionele vrijheid om de ernst van de situatie te beoordelen wordt genomen, komt duidelijk naar voren in de volgende toelichting: "*Op de meeste vragen dient een genuanceerd antwoord gegeven te worden. Vermoeden van criminaliteit kan op verschillende manier aan de hand zijn: plannen van een moord op iemand is nogal wat anders dan de planning om een pakje kauwgom te stelen.*"

[471] Art. 7.3.2 lid 3 en 7.3.11 lid 4 Jeugdwet.

[472] Idem.

[473] Idem.

Ten slotte geven professionals en ambtenaren in de toelichtingsmogelijkheden van de enquête aan dat bij dit soort situaties veel wordt overlegd binnen het team en met de leidinggevende. Een voorbeeld*: "Hangt ervan af is ingevuld omdat elke situatie goed gewogen moet worden, en in overleg met leidinggevende".*

Mag wel en mag niet
Bij de tweede optie zien we veel tegenovergestelde meningen. Deze situaties voldoet aan geen van de eerder gestelde criteria. Hiertoe behoren de volgende situaties: vermoeden van fraude, vermoeden van criminaliteit, overlast voor de omgeving, veiligheid van (volwassen) cliënt en bij een informeel signaal dat iemand mogelijk hulp nodig heeft. Bij de situaties waar verschillend op wordt gereageerd spreken we niet van een praktijknorm. Professionals en ambtenaren hebben in deze gevallen te uiteenlopende meningen.

Weet het niet
Ten slotte is er de mogelijkheid dat professionals en ambtenaren "niet weten" wat ze in die situatie zouden doen. De praktijksituaties die we in de enquête hebben voorgelegd roepen niet bij veel ondervraagden die reactie op. In de focusgroep werden wel twee van deze situaties beschreven. De eerste betrof de top-600. Een teamleider noemt de samenwerking met het meldpunt overlast en bij situaties in het kader van de top-600 als omstandigheden wanneer van regels kan worden afgeweken. De gemeente geeft toestemming voor het melden van een adres, of slachtoffer, maar de cliënt weet dit dan niet. Hetzelfde geldt voor situaties waarin de hulpverlening aan een cliënt is gestopt. Iemand vraagt of de politie moet worden ingelicht als bekend is dat een voormalige cliënt een vuurwapen draagt.

De tweede situatie gaat over radicalisering. Niet alle hulpverleners hebben ervaring met (het herkennen van) radicalisering en ze vragen zich af hoe ze in dergelijke situaties moeten optreden. Men is het erover eens dat als het zichtbaar is dat er echt iets aan de hand is, optreden noodzakelijk is. Maar wat hulpverleners moeten doen bij een vermoeden van radicalisering is onduidelijk. Het wordt nog lastiger als het om een gezinslid gaat dat niet bij de oorspronkelijke hulpvraag is betrokken, zoals een kind dat naar Syrië gaat of terugkomt.

7.3.3 Conclusie
De 12 praktijkvoorbeelden laten zien dat het resultaat van de belangenafweging bij verschillende situaties verschillende uitkomsten kent. In sommige gevallen zijn de ondervraagden het erg met elkaar eens. Uit de enquête blijkt dat bij 4 van de 12 praktijksituaties dat het geval is. Professionals en ambtenaren zijn van mening dat delen wel mag in de situatie dat de veiligheid van het kind in het geding is. En gegevens mogen niet gedeeld worden in situaties dat de betrokkene de Nederlandse taal niet machtig is, het delen van gegevens voor een efficiëntere informatieuitwisseling zorgt en het delen een betere dienstverlening aan de betrokkene oplevert.

In deze situaties lijkt er een praktijknorm te zijn ontstaan waarbij professionals en ambtenaren consistent handelen.

Ondervraagden zijn soms ook verdeeld. Dat kan op verschillende manieren. Allereerst zijn er praktijksituaties waarbij veel ondervraagden van mening zijn dat het wel of niet delen van gegevens afhangt van de specifieke omstandigheden. Dit zien we bij zorgmijdend gedrag, gezondheidsrisico's voor de betrokkene en als de betrokkene een verstandelijke of geestelijke beperking heeft. De professionals en ambtenaren lijken hier de praktijknorm te hanteren dat in dit soort gevallen een zekere professionele vrijheid nodig is. In de tweede plaats zijn er situaties waarin de ondervraagden wel een uitgesproken mening hebben, maar die mening verschilt onderling. In dit geval ontbreekt een praktijknorm. Hiertoe behoren de volgende situaties: vermoeden van fraude, vermoeden van criminaliteit, overlast voor de omgeving, veiligheid van (volwassen) cliënt en bij een informeel signaal dat iemand mogelijk hulp nodig heeft. Tenslotte is mogelijk dat professionals en ambtenaren echt niet weten hoe ze moeten handelen. In de focusgroep werden als voorbeelden het uitwisselen van gegevens over de top-600 jongeren en het uitwisselen van gegevens over jongeren waarbij sprake lijkt te zijn van radicalisering, genoemd.

7.4 Conclusie

In dit hoofdstuk stond de vraag centraal: *Wat is balans tussen privacy en gegevensverwerking in de praktijk*. Om deze vraag te beantwoorden hebben we allereerst gekeken welke randvoorwaarden professionals en ambtenaren passend vinden om een belangenafweging te maken tussen een adequate gegevensverwerking en respectvolle omgang met privacy. Voor de belangenafweging zijn de randvoorwaarden essentieel voor het waarborgen van privacy en het efficiënt en effectief uitvoeren van de werkzaamheden. Wanneer de randvoorwaarden op orde zijn is het makkelijker om deze belangenafweging te maken. De professionals en ambtenaren zijn positief over de aandacht van de organisatie voor privacy. De scholingsmogelijkheden vinden de professionals echter wel te beperkt. Ook maken professionals en ambtenaren kanttekeningen bij andere randvoorwaarden: de privacyregelgeving belemmert de werkzaamheden, de functionaliteit van RIS is onvoldoende, ze denken dat de autorisatie tot dossiers in RIS te ruim is en de dossiervorming kan zorgen voor een bovenmatige gegevensverzameling. Wij verwachten dat deze omstandigheden een goede hulpverlening aan de betrokkene bemoeilijken.

Daarnaast hebben we aan de hand van een aantal praktijksituaties geanalyseerd waarin de belangenafweging die professionals en ambtenaren bij het delen van gegevens maken, resulteert. We signaleren in de onderzochte praktijksituaties twee soorten uitkomsten van belangenafwegingen. Bij de eerste uitkomst zien we dat eensgezindheid tussen de professionals en ambtenaren over de vraag of gegevens wel of niet gedeeld mogen worden. Deze gevallen bestempelen we als praktijknormen

omdat professionals en ambtenaren consistent handelen. Zo is circa 80% van mening dat gegevens gedeeld mogen worden als de veiligheid van het kind in het geding is.

Bij de tweede soort uitkomst van belangenafweging zien we een grote mate van verdeeldheid tussen professionals en ambtenaren of gegevens wel of niet gedeeld mogen worden. We onderscheiden hierbij drie soorten situaties. Allereerst situaties waarbij ongeveer de helft van de professionals en ambtenaren van mening is dat het wel of niet delen van gegevens van de situatie afhangt. Dit is in zekere zin ook een praktijknorm omdat de professionals en ambtenaren consistent van mening zijn dat het wel of niet delen van gegevens in deze situaties afhankelijk is van de context. In de focusgroep werd bijvoorbeeld aangegeven dat het bij zorgmijdend gedrag sterk afhangt van de contex: als de risico's voor de betrokkene en/of de omgeving te groot worden (context), vinden professionals en ambtenaren dat gegevens gedeeld mogen worden. Bij het tweede type situatie zien we dat professionals en ambtenaren verschillend reageren op de situatie. In dit geval is er geen praktijknorm. We zien dit bijvoorbeeld terug bij fraude en criminaliteit. Ten slotte bestaan er situaties dat professionals en ambtenaren echt niet weten of ze gegevens zouden delen. In de focusgroep werden als voorbeelden genoemd het delen van kennis van jongeren uit de top-600 en jongeren waarbij signalen van radicalisering zichtbaar zijn.

Deze variatie in reacties vraagt om een verdere ondersteuning van de professionals en ambtenaren voor het maken van belangenafwegingen in deze en andersoortige situaties.

8 Enquête burgerpanel

8.1 Inleiding

De vorige hoofdstukken geven inzichten over hoe de gemeente omgaat met het vraagstuk van gegevensverwerking en het waarborgen van de privacy van de burgers in het sociaal domein. Dat gaat zowel over de afspraken die zijn gemaakt als over de uitvoering door en de ervaringen van professionals en ambtenaren in de praktijk. In dit hoofdstuk verleggen wij het perspectief naar de burger. Dit doen we aan de hand van een vragenlijst waarin we onderdelen uit het rapport hebben voorgelegd aan ons rekenkamerpanel. De betrokkenheid van het rekenkamerpanel vinden we zeker bij dit onderwerp belangrijk. Het panel heeft namelijk privacy als onderwerp aangedragen voor het publieksonderzoek 2015 van de rekenkamer.

De vraag die in dit hoofdstuk centraal staat, luidt:

Hoe kijkt de burger aan tegen het opslaan en delen van privacygevoelige gegevens door of namens de gemeente?

Om deze vraag te beantwoorden bekijken we allereerst het oordeel van het burgerpanel over de mate waarin de gemeente zorgvuldig omgaat met hun gegevens (paragraaf 8.1) Vervolgens gaan we in op de mening van het burgerpanel over de volgende drie onderdelen van gegevensverwerking: welke gegevens panelleden nodig achten in verschillende situaties (paragraaf 8.2), de manier waarop panelleden voorgelicht willen worden over gegevensverwerking (paragraaf 8.3) en in welke situaties panelleden van mening zijn dat gegevens gedeeld mogen worden zonder vooraf toestemming te vragen aan de burger met een hulpvraag (paragraaf 8.4).

In de vragenlijst worden vragen gesteld over situaties waar professionals en ambtenaren in het sociaal domein mee te maken hebben.[474] Dit zijn situaties die de panelleden waarschijnlijk niet uit eigen ervaring kennen en waarvan het (mogelijk) ook lastig is om zich een voorstelling van te kunnen maken. Sommige burgerpanelleden hebben ook aangegeven dat ze moeite hadden met het beantwoorden van sommige vragen. Dit begrijpen wij en daar hebben we ook rekening mee gehouden in onze analyse. Toch geeft de analyse naar ons idee wel interessante inzichten, die wij een waardevolle toevoeging vinden voor dit onderzoek.

[474] Het afgelopen jaar hebben we het burgerpanel meermaals om hun mening gevraagd over het onderwerp Privacy voor Burgers. In dit hoofdstuk volgen wij in grote lijnen de laatste vragenlijst die we aan het burgerpanel hebben voorgelegd. Deze vragenlijst was volledig gericht op dit onderzoek. De vragenlijst is op 8 februari 2016 verzonden naar het rekenkamerpanel en op 15 februari is de enquête weer gesloten. Aan het onderzoek hebben 824 panelleden deelgenomen. De vragenlijst bestond uit 4 onderdelen: (1) algemeen beeld van gegevens, (2) opvragen en vastleggen van gegevens, (3) voorlichten van gegevens en (4) delen van gegevens.

8.2 Belang van zorgvuldige omgang met gegevens

In deze paragraaf bespreken we het belang dat burgerpanelleden hechten aan een zorgvuldige omgang met hun gegevens en het vertrouwen dat ze hebben dat de gemeente ook deze zorgvuldigheid betracht. Om het oordeel over de gemeente enig reliëf te geven vergelijken we dat oordeel met het oordeel over drie andere organisaties: webwinkels, sociale media en huisartsen. In tabel 8.1 staan de resultaten samengevat voor het belang dat de panelleden hechten aan een zorgvuldige omgang met hun gegevens en het vertrouwen dat ze er in hebben dat er ook daadwerkelijk sprake is van een zorgvuldige omgang met gegevens.[475]

Tabel 8.1 - *Zorgvuldig omgaan met gegevens die organisaties opslaan (op basis van belang en vertrouwen)*

	Belang	Vertrouwen			
	(zeer) belangrijk	(zeer) weinig vertrouwen	Neutraal	(zeer) veel vertrouwen	N
Webwinkels	91,8%	65,0%	25,6%	6,4%	824
Gemeenten	97,3%	15,7%	36,5%	46,8%	824
Sociale media	88,8%	79,4%	14,1%	3,9%	824
Huisartsen	97,1%	5,8%	17,7%	75,6%	824

Overal wordt het belang van een zorgvuldige omgang met gegevens groot geacht. De variatie tussen organisaties is niet erg groot. De score voor de gemeente is hoog (97,3%). Vergelijkbaar met de huisarts (97,1%). Aan de zorgvuldige omgang met de gegevens door webwinkels en sociale media wordt door iets minder panelleden belang gehecht (maar nog steeds vindt 91,8% respectievelijk 88,8% het (zeer) belangrijk).

De mate dat de panelleden vertrouwen dat de verschillende organisaties zorgvuldig omgaan met persoonsgegevens zorgt wel voor een gevarieerde beoordeling. Bijna de helft van het panel heeft veel vertrouwen in de gemeente. Een derde reageert neutraal. De huisartsen scoren duidelijk beter. Circa 75% van de ondervraagden geeft aan (zeer) veel vertrouwen te hebben dat huisartsen zorgvuldig met hun gegevens omgaan. De panelleden hebben weinig vertrouwen in de sociale media (79,4% heeft (zeer) weinig vertrouwen) en webwinkels (65,0% heeft (zeer) weinig vertrouwen).

De panelleden geven aan dat ze het belangrijk vinden dat gemeenten goed omgaan met hun gegevens. Dit geldt overigens ook voor andere organisatie. De helft van panelleden geeft aan vertrouwen te hebben in de zorgvuldigheid waarmee gemeenten met gegevens omgaan. Dit aantal is groter dan bij webwinkels en de sociale media, maar minder dan bij huisartsen.

[475] In een eerdere enquête (december 2015) hebben we dezelfde vraag gesteld maar dan voor 13 organisaties. Het beeld dat in deze paragraaf wordt geschetst voor de vier organisaties, komt overeen met de resultaten van de eerdere enquête.

8.3 Opvragen en vastleggen van gegevens

De gemeente Amsterdam en de zorginstellingen waarmee ze samenwerkt slaan veel persoonsgegevens op van burgers met een hulpvraag. Dat mag alleen voor zo ver dat noodzakelijk is voor een goede hulpverlening aan de betrokkene. Afwegingen zijn voor de professionals en ambtenaren vaak lastig en protocollen en werkwijzers schieten soms te kort.

Professionals van Samen DOEN en Wijkzorg[476] worden gestimuleerd om gegevens van burgers met een hulpvraag te registreren aan de hand van de leefdomeinen van de zelfredzaamheidsmatrix (zie paragraaf 5.4.4). Daardoor kan men teveel persoonsgegevens gaan vragen, opslaan en delen. We vinden het risico op bovenmatig registreren bij Samen DOEN en Wijkzorg groot.

Situaties waarbij gegevens worden opgevraagd en vastgelegd
Het leek ons informatief om na te gaan welke persoonsgegevens leden van het burgerpanel in verschillende situaties nodig achten om op te vragen en vast te leggen. De voorgelegde situaties zijn gebaseerd op de hulpverlening van Samen DOEN, OKT en Wijkzorg. De situaties zijn: ondersteuning in het geval dat er sprake is van schulden, een licht verstandelijke beperking en werkloosheid (Situatie 1: Samen DOEN), verzoek voor het krijgen van een cursus voor een kind over hoe om te gaan met gedragsproblemen (Situatie 2: OKT) en aanvragen van huishoudelijk hulp (Situatie 3: Wijkzorg). De persoonsgegevens die wij het panel ter overweging geven, zijn ontleend aan de zelfredzaamheidsmatrix.[477]

Bij de beschrijving van de uitkomsten onderscheiden we drie categorieën. We beschouwen persoonsgegevens als *nodig* volgens het panel voor de dienstverlening als meer dan de helft van de ondervraagden dit aangeeft. We vinden het panel *onzeker* als een derde tot de helft zegt dat dit nodig lijkt voor de dienstverlening. Als minder dan een derde het nodig vindt, typeren we dat als *niet nodig* volgens het panel.

Inbeelden van situaties
Het was voor de burgerpanelleden soms lastig om zich een goede voorstelling van de situaties te maken. Een burgerpanellid geeft aan dat het moeilijk is om de vragen in te vullen omdat het niet zijn/haar werkterrein is: "*Heel lastig om in te vullen. Je kan vaak niet overzien wat de gevolgen van een uitspraak zijn, omdat dit niet je werkterrein is*". Een andere burgerpanellid zegt eigenlijk meer tijd nodig te hebben voor een goed oordeel: "*Ik vind dit eigenlijk onderwerpen waar ik dagen over zou moeten nadenken om er een goed antwoord op te hebben […]*". Zoals aangegeven in de inleiding van dit hoofdstuk begrijpen wij deze opmerkingen. We wilden echter toch graag een indruk van de mening van de burger over de situaties waarin de professional zichzelf een mening moet vormen.

---

[476] Voor zover het ambulante ondersteuning of dagbesteding betreft

[477] De te kiezen persoonsgegevens staan aangegeven in de tabellen. Overigens wordt bij OKT de ZRM zelden uitgevraagd. Zie ook voetnoot 485

Situatie 1: Samen DOEN
In de eerste situatie beschrijven we een burger met een hulpvraag die ondersteuning nodig heeft van Samen DOEN omdat er sprake is van schulden, een licht verstandelijke beperking en werkloosheid. Dit is kenmerkend voor Samen DOEN; de hulpvraag heeft meestal te maken met verschillende problemen. Hiervoor zijn in het algemeen meerdere gegevens van belang.

Het burgerpanel is in deze situatie bij veel gegevens onzeker over de noodzaak om gegevens te registreren (tabel 8.2). Het inkomen (82,4%), Burgerservicenummer (77,8%) en de geestelijke gezondheid (60,8%) vinden de ondervraagden *nodig* voor de dienstverlening. Dit beeld van de burger wijkt af van de protocollen en werkwijzers van Samen DOEN. Hierin wordt vereist dat in RIS voor alle leefdomeinen van ZRM gegevens worden opgevraagd en vastgelegd. Maar de mening van de panelleden staat daar ook niet echt haaks op. Er heerst onder het burgerpanel veel *onzekerheid,* maar geen van de persoonsgegevens vinden de ondervraagden *niet nodig*.

Tabel 8.2 - *Gegevensbehoefte bij een situatie typerend voor Samen Doen*

Persoonsgegevens	% dat gegevens nodig acht
Burgerservicenummer	77,8
Inkomen	82,4
Geestelijke gezondheid	60,8
Verslaving	43,2
Justitie	36,3
Dagbesteding	34,8
Gezinsrelaties	42,4
Fysieke gezondheid	35,0
Ouderschap	37,1
Geen enkele informatie	3,8
Weet ik niet	7,5
N	*824*

Situatie 2: OKT
In de tweede situatie gaat het over een burger met een hulpvraag die bij OKT terecht komt voor een verzoek voor het krijgen van een cursus voor een kind over hoe om te gaan met gedragsproblemen. Volgens het panel zijn voor deze situatie alleen de gegevens over ouderschap (60,2%) *en* de gegevens over gezinsrelaties (55,8%) nodig (tabel 8.3). Over het Burgerservicenummer (45,6%) en de geestelijke gezondheid (37,6%) twijfelt men. Het panel vindt de overige gegevens niet nodig voor de hulpverlening.

Bij OKT is het niet verplicht om alle gegevens uit de zelfredzaamheidmatrix in te vullen en te registreren in RIS (zie hoofdstuk 6).[478] De panelleden laten wel een duidelijk beeld zien welke gegevens (uit de zelfredzaamheidmatrix) zij relevant vinden voor de registratie. Dit zijn vooral ouder- en kindgerelateerde gegevens.

Tabel 8.3 - *Gegevensbehoefte bij een situatie typerend voor OKT*

Persoonsgegevens	% dat gegevens nodig acht
Burgerservicenummer	45,6
Inkomen	29,6
Geestelijke gezondheid	37,6
Verslaving	25,4
Justitie	22,9
Dagbesteding	13,8
Gezinsrelaties	55,8
Fysieke gezondheid	14,8
Ouderschap	60,2
Geen enkele informatie	13,6
Weet ik niet	6,7
N	824

Situatie 3: Wijkzorg
In de derde situatie gaat het over een burger met een hulpvraag die huishoudelijke hulp aanvraagt. Voor een dergelijke aanvraag zal de burger terecht komen bij Wijkzorg. Uit de enquête blijkt dat het panel alleen de volgende gegevens *nodig* vindt voor de hulpverlening (tabel 8.4): fysieke gezondheid (73,4%), inkomen (70,8%) en Burgerservicenummer (61,5%). Alle andere gegevens vinden de respondenten *niet nodig* voor de dienstverlening. Dit is een scherper contrast dan bij de situaties 1 en 2. De onzekerheid is met andere woorden minder groot.

Voor het aanvragen van WMO-voorzieningen (zoals huishoudelijke hulp, een traplift of woon- en vervoersvoorzieningen) leggen professionals van Wijkzorg geen gegevens vast in RIS, maar in het registratiesysteem Wmo-ned. Voor deze voorzieningen hoeft geen verplichte ZRM afgenomen te worden. Deze werkwijze past bij het beeld dat de burger heeft bij deze situatie.

Tabel 8.4 – *Gegevensbehoefte bij een situatie typerend voor Wijkzorg*

Persoonsgegevens	% dat gegevens nodig acht
Burgerservicenummer	61,5
Inkomen	70,8
Geestelijke gezondheid	26,9
Verslaving	10,0

[478] In de enquête aan de professionals en ambtenaren van de RIS-modules Samen DOEN, OKT en Wijkzorg hebben enkele ondervraagden van OKT aangegeven wel de ZRM in te vullen.

Persoonsgegevens	% dat gegevens nodig acht
Justitie	4,9
Dagbesteding	13,6
Gezinsrelaties	22,6
Fysieke gezondheid	73,4
Ouderschap	6,1
Geen enkele informatie	5,8
Weet ik niet	5,2
N	824

8.4 Voorlichting over gegevensverwerking

In de privacyprotocollen van Samen DOEN, Wijkzorg en OKT staat expliciet beschreven dat de professional uitlegt hoe hij/zij moet omgaan met persoonsgegevens, welke rechten betrokkenen hebben en dat betrokkenen actief moeten worden geïnformeerd. De panelleden hebben in een eerdere enquête ook aangegeven graag te grip te hebben op hun gegevens.[479] In deze enquête is aan het burgerpanel gevraagd of ze voorgelicht willen worden wie informatie heeft en controle willen hebben wie hun gegevens kunnen inzien (tabel 8.5). De panelleden hebben duidelijk aangegeven graag te weten welke personen beschikken over informatie over hen (92,2% vindt dit (heel) belangrijk). Ook geeft het panel aan graag controle te hebben over welke personen hun gegevens kunnen inzien (93,0% vindt dit (heel) belangrijk). Kortom, de panelleden willen graag grip houden op hun gegevens.

Tabel 8.5 -*Voorlichting en controle wie inzage heeft tot gegevens*

Kunt u aangeven hoe belangrijk u het vindt om:	(helemaal) niet belangrijk	Neutraal	(heel) belangrijk	Weet niet	N
Te weten wie informatie over u heeft	1,8%	5,9%	92,2%	0,1%	733
Controle te hebben over wie uw gegevens kan inzien	1,4%	5,3%	93,0%	0,3%	733

Informeren via meerdere kanalen
De burger wordt voorgelicht via meerdere kanalen: website, folder, brieven en mondeling (paragraaf 6.3). Dat is positief. Wel hebben we geconstateerd dat folders niet altijd worden meegegeven en de voorlichting niet altijd volledig is. Daarnaast blijkt uit de enquête onder professionals en ambtenaren dat burgers met een hulpvraag niet altijd geïnformeerd worden over hun rechten (paragraaf 6.6).

[479] Deze enquête is begin december verstuurd naar het Rekenkamerpanel. Aan dit onderzoek hebben 733 panelleden deelgenomen.

In de vragenlijst hebben we de leden van het burgerpanel gevraagd hoe ze geïnformeerd willen worden over welke gegevens worden opgeslagen, met wie en op welk moment deze gegevens worden gedeeld en welke rechten ze hebben. De burgerpanelleden hebben aangegeven vooral voorgelicht te willen worden door middel van een brief voorafgaand aan de eerste hulpverlening (70,1%) en via de website (63,7%). Minder populair is een folder (33,0%) en mondelinge voorlichting (22,3%). De overige panelleden geven aan niet te weten (2,5%) hoe ze willen worden voorgelicht.

De panelleden laten een duidelijke voorkeur zien voor de brief en de website. Omdat in de praktijk het vragen om toestemming meestal wordt gekoppeld aan toelichting gebeurt het vaak mondeling (paragraaf 6.4). Dit verschil met de wensen van het panel, is wel een punt van aandacht. Wellicht prefereert men brief of website omdat er dan rustiger over nagedacht kan worden en niet met de vraag overvallen wordt.

8.5 Delen van gegevens

Aan de professionals en ambtenaren hebben we ook 12 concrete praktijksituaties voorgelegd waarin aangegeven moest worden of gegevens gedeeld mogen worden *zonder toestemming* van de cliënt. Omdat we ook graag wilden weten hoe burgers hier tegen aankijken, hebben we dezelfde 12 situaties ook aan het burgerpanel voorgelegd.

Net als bij andere onderdelen van de enquête is deze vraag lastig gebleken. Een panellid maakt duidelijk zich niet goed een voorstelling van de situatie te kunnen maken: *"Omdat ik niet weet in welke mate wie welke informatie wel of niet zou delen, vind ik het moeilijk om daarop een goed antwoord te geven."* Een ander panellid kon zich geen beeld vormen van met wie er dan informatie zou moeten worden gedeeld "D*e laatste vraag vond ik niet duidelijk. Wie delen er de informatie?"*. Deze situaties zijn inderdaad lastig te interpreteren als je er niet dagelijks mee te maken hebt. De analyse levert echter ook bij dit onderdeel toch interessante inzichten op.

Aanpassen categorieën
Bij de situaties die aan de professionals en ambtenaren zijn voorgelegd kon een keuze gemaakt worden tussen 'wel delen', 'niet delen', 'hangt er van af' en 'weet ik niet'. Voor de enquête aan ons burgerpanel hebben we de 'hangt er van af'-categorie opgedeeld in 'hangt er van af, maar ik neig naar delen mag' en 'hangt er van af, maar ik neig naar delen mag niet'. Door deze aanpassing zijn de resultaten minder goed één-op-één vergelijkbaar met de resultaten van de professionals en ambtenaren. Wel heeft deze opdeling de resultaten naar ons idee beter inzichtelijk gemaakt. In onze analyse onderscheiden we de situaties waarin de meerderheid van het burgerpanel neigt naar wel delen van gegevens en situaties waarin het burgerpanel neigt naar niet delen van gegevens.

(Hangt er van af maar ik neig naar) wel delen
Uit de enquête blijkt dat in een aantal situaties de meerderheid van de ondervraagden van mening is dat gegevens gedeeld mogen worden zonder toestemming van de burger met een hulpvraag (tabel 8.6). Net als de professionals en ambtenaren vinden burgers de veiligheid van kinderen (89,1%) de belangrijkste reden om gegevens te delen zonder toestemming van de cliënt. Bij het vermoeden van criminaliteit en het vermoeden tot fraude is de meerderheid van mening dat het delen van gegevens acceptabel is (circa 80%). In het geval van zorgmijdend gedrag, cliënten met een verstandelijke/geestelijke beperking en bij gezondheidsrisico's voor de cliënt heeft de meerderheid (circa tweederde) de neiging gegevens te delen zonder toestemming van cliënt. Het burgerpanel vindt in deze zorggerelateerde situaties het delen van gegevens meer van de situatie afhangen.

De resultaten van het burgerpanel laten een ander beeld zien dan we hebben gezien bij de professionals en ambtenaren. De laatstgenoemde groep is alleen eensgezind dat gegevens gedeeld mogen worden bij de veiligheid van kinderen. De burgers lijken iets soepeler over het delen dan de professionals en ambtenaren. Zij vinden in meer situaties het delen van gegevens acceptabel. Deze situaties zijn vooral gerelateerd aan veiligheid en zorg. Het is mogelijk dat de verschillende uitkomsten te maken hebben met de iets andere vorm waarin wij de vraag hebben voorgelegd aan het panel. Deze vorm biedt bij twijfel toch de mogelijkheid om een (lichte) voorkeur kenbaar te maken.

Tabel 8.6 - *Situaties waarin de meerderheid van mening is dat het acceptabel is dat de professional of ambtenaar gegevens deelt zonder toestemming van cliënt*

	Delen mag wel (A)	Hangt er vanaf, maar ik neig naar "delen mag" (B)	*Totaal (A+B)*	*N*
Veiligheid van kinderen	59,7%	29,4%	89,1%	817
Vermoeden dat de cliënt fraudeert	44,6%	34,9%	79,5%	817
Vermoeden van criminaliteit, anders dan fraude	49,9%	29,1%	79,0%	817
Veiligheid van cliënt (geen kind)	26,6%	40,8%	67,4%	817
Zorgmijdend gedrag	19,8%	43,9%	63,3%	817
Cliënten met een verstandelijke/geestelijke beperking	22,4%	40,6%	63,0%	817
Gezondheidsrisco's voor de cliënt	22,8%	40,1%	62,9%	817
Overlast voor de omgeving van de cliënt	23,4%	37,3%	60,7%	817
Een informeel signaal van een buitenstaander dat iemand mogelijk hulp nodig heeft	11,9%	39,4%	51,3%	817

(Hangt er van af maar ik neig naar) niet delen
Voor de overige situaties is het burgerpanel van mening dat het delen van gegevens zonder toestemming van de cliënt niet acceptabel is (tabel 8.7). Dit zijn dezelfde situaties waarover de professionals en ambtenaren eensgezind zijn dat gegevens niet gedeeld mogen worden. Situaties waarbij de meerderheid van het burgerpanel van mening is dat gegevens niet gedeeld mogen worden zijn: efficiënte informatie-uitwisseling (62,1%), betere dienstverlening aan de cliënt (61,1%) en in het geval dat de cliënt de Nederlandse taal niet machtig is (54,2%). Deze situaties hebben, in tegenstelling tot situaties waarbij de meerderheid van het burgerpanel wel mening is dat gegevens gedeeld mogen worden, niet met de veiligheid of de zorgbehoefte van de cliënt te maken.

Tabel 8.7 - *Situaties waarin de meerderheid van mening is dat het niet acceptabel is dat de professional of ambtenaar gegevens deelt zonder toestemming van cliënt*

	Delen mag niet (A)	Hangt er vanaf, maar ik neig naar "delen mag niet" (B)	*Totaal (A+B)*	*N*
Efficiënte informatie uitwisseling	38,7%	24,0%	62,1%	816
Betere dienstverlening aan de cliënt	38,1%	23,0%	61,1%	817
Cliënten die Nederlandse taal niet machtig zijn	33,5%	20,7%	54,2%	817

8.6 Conclusie

Hoe de burger aankijkt tegen het opslaan en delen van privacygevoelige gegevens?

Panelleden geven aan dat ze het (zeer) belangrijk (97,3%) vinden dat gemeenten goed omgaan met hun gegevens. Hetzelfde geldt voor webwinkels, sociale media en huisartsen. De mate waarin de panelleden vertrouwen dat verschillende organisaties zorgvuldig omgaan met persoonsgegevens zorgt wel voor een gevarieerde beoordeling. Ongeveer de helft van de panelleden geeft aan vertrouwen te hebben in de zorgvuldigheid waarmee gemeenten met gegevens omgaan en een derde reageert neutraal. In webwinkels ((zeer) weinig vertrouwen 65,0%) en sociale media ((zeer) weinig vertrouwens 79,4%). Huisartsen scoren duidelijk beter ((zeer) veel vertrouwen 75,6%).

De leden van ons burgerpanel geven aan van welke gegevens – ontleent van de zelfredzaamheidsmatrix (ZRM) – zij het in verschillende situaties logisch vinden dat de gemeente of instellingen deze opvragen om hulp te kunnen verlenen. Het ging hier om gegevens zoals burgerservicenummer, inkomen, geestelijke gezondheid,

gezinsrelaties en fysieke gezondheid. We vatten de resultaten voor de drie situaties hieronder samen:

- Situatie 1: Ondersteuning als er sprake is van schulden, een licht verstandelijke beperking en werkloosheid (Samen Doen). Het panel vindt informatie over inkomen (82,4%), burgerservicenummer (77,8%) en de geestelijke gezondheid (60,8%) nodig.
- Situatie 2: Verzoek voor het krijgen van een cursus voor een kind over hoe om te gaan met gedragsproblemen (OKT). Het panel vindt informatie over ouderschap (60,2%) en de gegevens over gezinsrelaties (55,8%) nodig. Over het Burgerservicenummer (45,6%) en de geestelijke gezondheid (37,6%) twijfelt men.
- Situatie 3: Aanvragen van huishoudelijke hulp (Wijkzorg). Het panel vindt informatie over fysieke gezondheid (73,4%), inkomen (70,8%) en Burgerservicenummer (61,5%) nodig.

Panelleden geven aan het (heel) belangrijk (92,2%) te vinden om te weten welke personen informatie over hen hebben opgeslagen en vinden het (heel) belangrijk (93,0%) controle te hebben over welke personen hun gegevens kunnen inzien. De burgerpanelleden willen dat de gemeente en de instellingen hen voorlicht door middel van een brief voorafgaand aan de eerste hulpverlening (70,1%) en via de website (63,7%). Minder populair is een folder (33,0%) en mondelinge voorlichting (22,3%).

Ten slotte hebben we aan de hand van een aantal praktijksituaties geanalyseerd wanneer de panelleden het acceptabel vinden dat gegevens zonder toestemming van de cliënt gedeeld worden. We zien daarin drie patronen terug. Allereerst zien we een patroon bij situaties gerelateerd aan veiligheid. De meerderheid van de burgerpanelleden is bij deze situaties van mening dat gegevens gedeeld mogen worden. Dit zijn situaties zoals de veiligheid van kinderen en het vermoeden dat de cliënt fraudeert. Daarnaast zien we een patroon bij situaties die gerelateerd zijn aan de zorgbehoefte van cliënt. De meerderheid is van mening dat in deze situatie gegevens wel gedeeld mogen worden, maar dat ze het wel van de context vinden afhangen. Dit zijn situaties zoals zorgmijdend gedrag en cliënten met een verstandelijke/geestelijke beperking. Ten slotte zien we een patroon in de situaties waarbij panelleden het niet acceptabel vinden dat gegevens gedeeld worden. Het delen heeft in deze situaties een praktische reden, zoals een efficiënte informatie uitwisseling of cliënten die de Nederlandse taal niet machtig zijn.

9 Conclusie

In dit rapport hebben wij de afspraken, en de uitvoering daarvan, beschreven en beoordeeld op het borgen van privacy voor de onderdelen jeugd en zorg binnen het sociaal domein. Daarbij stond de vraag centraal of zich een praktijk ontwikkelt waarin een balans wordt gevonden tussen een dusdanige gegevensverwerking waardoor de hulpverlening kan worden gegeven en het respecteren van de privacy van de burger die bij deze hulpverlening is betrokken.

Het onderwerp privacy kende het laatste jaar een toenemende aandacht van het gemeentebestuur. Dit komt tot uiting in de notitie van het college '"Wat doet u met mijn gegevens?" Zorg voor de privacy'(januari 2015) en de begin 2016 aangekondigde maatregelen om de naleving van privacyregels te borgen. Het aantal raadsvragen van de gemeenteraadsleden van Amsterdam laat een stijgende politieke aandacht zien. Het belang van een goede omgang wordt ook door ons burgerpanel kenbaar gemaakt. Bijna ons gehele burgerpanel heeft aangegeven het (zeer) belangrijk (97,3%) te vinden dat gemeenten zorgvuldig omgaan met gegevens, maar de helft van het burgerpanel heeft er vertrouwen in dat gemeenten daadwerkelijk zorgvuldig omgaan met gegevens.

De transitie, transformatie en de gemeentebrede reorganisatie vroegen en vragen om continue aanpassing van beleid en de werkwijzen van ambtenaren en professionals. De voorbereiding op de transitie en transformatie en de start begin 2015 stonden in het teken van het continueren van bestaande en het garanderen van nieuwe hulpverlening aan hulpbehoevende Amsterdammers vanuit een integrale gedachte. In de loop van 2015 is er steeds meer aandacht gekomen binnen het sociaal domein voor privacy. De onderstaande conclusies moeten dan ook worden gelezen in de context van een zich continu ontwikkelend en lerend veld.

9.1 Actueel privacybeleid ontbreekt, het college beoogt prudent om te gaan met (bijzondere) persoonsgegevens

De gemeente, of in juridische zin het college van B en W, is verantwoordelijk voor de uitvoering van de verschillende taken en werkzaamheden uit de Jeugdwet en Wmo 2015. Daarmee is het college ook verantwoordelijk voor de gegevens die worden verwerkt van de bij de hulpverlening betrokken burgers. Dit geldt niet alleen als deze gegevens worden verwerkt door de gemeente zelf maar ook als deze worden verwerkt door een partij waarmee de gemeente samenwerkt of waaraan werk wordt uitbesteed. Deze systeemverantwoordelijkheid gaat verder dan de verantwoordelijkheid die het college heeft in de zin van de Wet bescherming persoonsgegevens (Wbp): om te zorgen dat gegevensverwerkingen aan de wet voldoen. De gemeente dient de regie te houden, ook als taken zijn uitbesteed. Juist daarom is het belangrijk dat het college beleid vaststelt waarin is aangegeven hoe het denkt over privacy, hoe het de privacy probeert te borgen in zijn eigen organisatie en bij samenwerkende

partijen en welke rol leren daarbij speelt.[480] Dit is van groot belang omdat privacy-regelgeving niet mag worden veronachtzaamd of terzijde worden geschoven, maar er niet de situatie mag ontstaan dat geen goede hulpverlening wordt gegeven, of erger, er levensbedreigende situaties ontstaan omdat de regels over gegevens-verwerking eenzijdig en/of beperkt worden uitgelegd.[481]

Het beleid voor het gebruik van persoonsgegevens voor de gehele gemeente is in 2009 voor het laatst herzien. Het college schetst daarin de visie dat informatie volledig, actueel, betrouwbaar, centraal en snel beschikbaar is en dat gegevensverwerking zo efficiënt en veilig mogelijk plaatsvindt met inachtneming van de privacywetgeving. Binnen deze visie op gegevensverwerking is privacy meer een randvoorwaarde. Een overkoepelende visie waarin privacy daadwerkelijk handen en voeten wordt gegeven, ontbreekt.

Privacybeleid voor het sociaal domein is niet opgesteld, maar voor de jeugdwet heeft het college in 2015 zijn ambities geformuleerd en de intentie uitgesproken dat deze voor het gehele sociaal domein zullen gaan gelden. Het college wil in beeld brengen welke gegevens wel en niet mogen worden verwerkt en worden gedeeld, zodat de handelingsbekwaamheid bij de uitvoerder en het vertrouwen van de burger in de overheid wordt vergroot. In een later stadium heeft het college aangegeven alleen die gegevens te willen opslaan die nodig zijn voor een goede hulpverlening en regelmatig te willen beoordelen of dit ook het geval is. Tevens wil het de toegankelijkheid tot dossiers voor ambtenaren en professionals beperken en wil het college het lerend vermogen vergroten door mensen meer op te leiden, te trainen en regelmatig lastige casuïstiek te laten bespreken. Uit deze visie spreekt de intentie voor het prudent om willen gaan met (bijzondere) persoonsgegevens van bij de hulpverlening betrokken burgers. Bovendien geeft het ambtenaren en professionals richting om tijdens de hulpverlening de afweging te maken hoe adequate hulpverlening kan worden gebonden terwijl de privacyregels worden gerespecteerd.

Het beleid uit 2009 is binnen de ambtelijke organisatie vrijwel onbekend en sluit onvoldoende aan bij de organisatiestructuur zoals deze per 2015 is ontstaan na de gemeentebrede reorganisatie van 2015 en wijze waarop nu wordt samengewerkt met instellingen. Recent privacybeleid ontbreekt, zowel op het gemeentelijke niveau als op het niveau van het sociaal domein. Hierdoor wordt voor de raad en de burger niet duidelijk hoe het college denkt over privacy en hoe zij er voor zorgt dat partijen waaraan taken zijn uitbesteed en waarmee de gemeente samenwerkt de privacy waarborgen, en hoe het daarop monitort en stuurt. Door het ontbreken van gemeenschappelijke uitgangspunten is het college ook weinig sturend bij de uitvoering van het beleid door ambtenaren en professionals.

[480] Zie Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, 7 november 2014, p 39.

[481] Zie ook Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, 7 november 2014, p. 4.

Zonder actueel beleid wordt verantwoording afleggen aan, en controle door, de gemeenteraad over de wijze waarop het college omgaat met privacy bemoeilijkt. Bovendien kan dit er onbedoeld toe leiden dat er binnen de organisatie, maar ook door samenwerkende partners, verschillend wordt omgegaan met privacyvraagstukken.[482]

9.2 De gemaakte afspraken dragen bij aan een goede toepassing van de privacyregels, maar privacy is met deze afspraken nog niet gewaarborgd

De gemeente is verantwoordelijk voor een adequate gegevensverwerking en een respectvolle omgang met privacy. Om deze verantwoordelijkheid waar te kunnen maken zijn zowel binnen de gemeente, als met de samenwerkende instellingen, vrijgevestigen en de softwareleverancier afspraken gemaakt. Deze afspraken dragen in opzet op hoofdlijnen bij aan het op een goede manier van omgaan van de privacy in de hulpverleningspraktijk. Toch zijn niet alle gemaakte afspraken van voldoende niveau om de privacy te waarborgen. We zien dit ook terug in de uitvoering van deze afspraken.

Verantwoordelijken voor beleidsvorming en -uitvoering privacybeleid nog onvoldoende helder
Zowel voor beleidsvorming als beleidsuitvoering geldt dat er veel organisaties en actoren bij betrokken zijn, zowel op bestuurlijk als ambtelijk niveau en zowel concernbreed als binnen het sociaal domein. Doordat taakomschrijvingen, verantwoordelijkheden en bevoegdheden van zowel organisaties als actoren niet volledig op elkaar aansluiten, niet geregeld of goed afgebakend zijn, ontstaat onduidelijkheid wie verantwoordelijk en aanspreekbaar is op het voldoen aan de privacyregelgeving en de gemeentebrede afspraken over privacy. Deze onduidelijkheid doet zich voor bij de vraag wie de regie heeft, wie toetst en wie monitort dat gegevensverwerkingen aan deze kaders voldoen. Ook kan deze onduidelijkheid eraan bijdragen dat van voorgeschreven kaders wordt afgeweken.

Kans op privacycompliance bij nieuwe gegevensverwerking is groter dan bij bestaande gegevensvwerking, maar geen garantie voor volledige privacycompliance
De kans dat wordt voldaan aan de privacyregelgeving uit de Wet bescherming persoonsgegevens of andere regelingen – de mate van privacycompliance – achten wij bij nieuwe gegevensverwerkingen groter dan bij bestaande gegevensverwerkingen, maar biedt geen garantie dat volledig aan regelgeving wordt voldaan.

Bij het ontwikkelen van nieuwe gegevensverwerkingen zijn de procedures zo ingericht dat er systematisch wordt nagedacht over het kunnen voldoen aan de privacyregelgeving. Ook is er structurele aandacht voor privacy- en beveiligingsrisico's en welke beheersmaatregelen moeten worden getroffen om deze te mitigeren. Het systeem is echter nog niet perfect, waardoor de kans bestaat dat niet altijd advies wordt ingewonnen of wordt opgevolgd.

[482] Zie ook Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, 7 november 2014

De aandacht voor privacy lijkt te verslappen zodra de nieuwe processen voor nieuwe gegevensverwerking zijn ingericht. Een structurele periodieke compliancetoets ontbreekt, waardoor voor bestaande gegevensverwerkingen niet structureel wordt nagegaan of deze (nog steeds) overeenkomstig de privacyregelgeving zijn. Het beschikbare instrumentarium – Wbp-monitor, incident- en datalekmeldingen en klachtenregistratie – is wel geschikt om incidentele afwijkingen te constateren, maar wordt niet benut om vast te stellen in hoeverre bestaande gegevensverwerkingen in lijn zijn met de privacyregelgeving.

De door ons onderzochte gegevensverwerkingen in het kader van de Jeugdwet (Samen DOEN en Ouder- en Kindteams) en Wmo 2015 (Wijkzorg) zijn alle drie aan te merken als nieuwe gegevensverwerkingen. De belangrijkste procedures zijn doorlopen waardoor er tijdens de ontwikkeling aandacht is geweest voor privacy en mogelijke risico's. Ook zijn beheersmaatregelen voorgesteld. De opvolging daarvan is niet gemonitord. De privacycoördinatoren zouden hierin, vanwege hun verantwoordelijkheid om privacy te borgen, een belangrijke taak moeten vervullen. In de praktijk maken ze die nog niet waar, als gevolg van tekortschietende bevoegdheden en onbekendheid binnen de organisaties met de privacycoördinatoren.

Afspraken met samenwerkende partijen op hoofdlijnen toereikend om privacy te waarborgen
Bij de uitvoering van de Jeugdwet en de Wmo 2015 werkt de gemeente met 119 gecontracteerde partijen en 167 vrijgevestigden samen, en maken circa 2.800 professionals en ambtenaren gebruik van de drie geautomatiseerde systemen waarin (bijzondere) persoonsgegevens van bij de hulpverlening betrokken burgers zijn opgeslagen.

De afspraken die de gemeente met deze partijen heeft gemaakt over het borgen van de privacy zijn grotendeels gelijkluidend en op hoofdlijnen in opzet toereikend om aan de privacyregelgeving te voldoen. Deze afspraken zijn vastgelegd in samenwerkings-, inkoop- en bewerkersovereenkomsten. Er ontbreken afspraken met Samen DOEN en Ouder- en Kindteams of het instellingen daarnaast is toegestaan om in eigen systemen (bijzondere) persoonsgegevens te verwerken. Tot slot zijn er geen afspraken gemaakt hoe de instellingen zich verantwoorden over de naleving van de gemaakte afspraken en welke toezichtsbevoegdheden de gemeente heeft om dit te controleren en eventueel te sanctioneren.

Gemaakte afspraken met softwareleverancier nog niet volledig gerealiseerd
De gemeente is de opdrachtgever voor de bouw van het Registratie Informatie Systeem (RIS). De (bijzondere) persoonsgegevens van, Samen DOEN, de Ouder- en Kindteams en Wijkzorg worden verwerkt in drie modules van RIS. Deze zijn niet aan elkaar zijn gekoppeld. De wijkteams gebruiken de modules voor het bijhouden van het cliënt- of het gezinsdossier, terwijl de gemeente dit gebruikt voor informatie ten behoeve van het beleid.

Met de softwareleverancier zijn afspraken gemaakt aan welke eisen van beveiliging, geheimhouding en het beschikbaar stellen van gegevens moet worden voldaan.

Wanneer naar de uitvoering van afspraken wordt gekeken, blijkt dat de borging van privacy nog niet helemaal in orde is. Niet alle afspraken tussen de gemeente en de softwareleverancier zijn nagekomen, terwijl de afgesproken datum daarvoor is verstreken. Zo ontbreekt het exitplan en is de uitwijklocatie nog niet operationeel, waardoor de continuïteit van de hulpverlening gevaar kan lopen. Ook heeft de softwareleverancier nog niet alle veiligheidscertificaten verkregen.

Autorisatie en gegevensbeveiliging redelijk op orde maar kan beter
De autorisaties in RIS zijn passend voor de functies, maar er zijn nog steeds veel functies en daarmee medewerkers die toegang hebben tot een cliëntdossier. Medewerkers van de softwareleverancier kunnen de (bijzondere) persoonsgegevens ook inzien. Toezicht hierop door de gemeente schiet tekort, waardoor niet wordt vastgesteld of en hoe vaak medewerkers onrechtmatig cliëntgegevens inzien,terwijl de gemeente hiervoor voldoende loggingsfaciliteiten beschikbaar heeft.
Daarnaast komt het voor dat (bijzondere) persoonsgegevens worden gedeeld via (onbeveiligde) mail, terwijl informatie-uitwisseling via een RIS-module zou moeten plaatsvinden.

Enkele ambtenaren hebben toegang tot cliëntgegevens
Volgens het college heeft de ambtelijke organisatie geen toegang tot zorginhoudelijke informatie. In de praktijk pakt dit anders uit. Voor Samen DOEN, waar teamleiders en teamassistenten ambtenaren zijn, hebben deze toegang tot de cliëntdossiers. Bovendien worden voor het vervaardigen van managementinformatie (bijzondere) persoonsgegevens gebruikt, zonder dat deze persoonsgegevens zijn geanonimiseerd.

Afspraken lerende organisatie dragen bij aan het waarborgen van de privacy
Zowel vanuit de gemeente als de instellingen waarmee de gemeente samenwerkt is aandacht voor een 'lerende praktijk'. Dit wordt ook beaamd door twee derde van de 552 ambtenaren en professionals die onze enquête hebben ingevuld. Zij zijn van mening dat er door hun organisatie voldoende aandacht aan privacy wordt besteed.

Op concernniveau is er beperkt aandacht voor privacy(bewustzijn). Een concernbrede bewustwordingscampagne staat gepland voor 2016. Binnen het cluster sociaal is het leren bij de ambtelijke organisatie en de instellingen erop gericht om het privacy-bewustzijn te ontwikkelen en verder te stimuleren. Daartoe worden verschillende opleidingen en cursussen aangeboden. Met uitzondering van de workshop voor de Ouder- en Kindteams en de trainingen voor het registratiesysteem, zijn deze niet nadrukkelijk gericht op privacy. Slecht een derde van de ambtenaren en professionals is van mening dat de scholingsmogelijkheden op orde zijn. De belangrijkste vraagbaken voor de hulpverleners bij privacyvraagstukken zijn de casuïstiek-overleggen, waar op basis van casussen het onderdeel privacy naar voren komt als gespreksonderwerp. Binnen Samen DOEN kunnen medewerkers daarnaast

terecht bij de privacycoördinator of aandachtsfunctionarissen voor hun vragen over privacy. Het is binnen het OKT en Wijkzorg nog onvoldoende gewaarborgd dat alle lessen die hierbij worden getrokken hun weg vinden in aanpassing van beleid en procedures. Bij Samen DOEN is dit met name door de werkgroep Privacy, waar hulpverleners onderdeel van uitmaken, beter georganiseerd.

Wij zien de meerwaarde van de privacyschouw van het jeugdstelsel voor het vergroten van het privacybewustzijn binnen de gemeente en de instellingen. Met de privacyschouw wordt, vanuit een burgerperspectief, de omgang met persoonsgegevens van burgers in beeld gebracht en getoetst. Daarbij moet worden opgemerkt dat de privacyschouw éénmalig is en beperkt is tot het jeugddomein.

College kondigt maatregelen aan voor naleving privacyregels
Halverwege januari 2016 heeft college van B en W aangegeven maatregelen te zullen treffen om de bewustwording over privacy bij medewerkers te zullen vergroten, de kaders voor het borgen van de taken en verantwoordelijkheden te zullen actualiseren, het toezicht op de naleving van privacywetgeving te versterken, de bewerkersovereenkomsten te actualiseren en te zullen anticiperen op nieuwe wetgeving.

9.3 Gemaakte privacy-afspraken vormen een goed startpunt om te bepalen of de gegevensverwerking passend is voor de hulpverlening. De afspraken zijn nog weinig sturend om bovenmatige gegevensverwerking te voorkomen.

De (privacy)afspraken tussen de gemeente en de instellingen over de algemene uitgangspunten, voorlichting hierover en de te doorlopen stappen bij de hulpverlening zijn geconcretiseerd in de privacyprotocollen. In opzet voldoen de privacyprotocollen van Samen DOEN, het OKT en Wijkzorg aan veel normen uit de Wbp, waaronder de voorlichting aan en het informeren van de betrokkene, de geheimhouding, het delen van gegevens, de termijnen voor inzage, correctie, vernietiging en bewaring van persoonsgegevens. De protocollen, in combinatie met werkwijzers en (de handleiding) RIS, bieden ambtenaren en professionals een startpunt om een goede afweging te maken welke (bijzondere) persoonsgegevens voor de hulpverlening noodzakelijk zijn om te verwerken terwijl daarbij de privacy van bij de hulpverlening betrokken burgers wordt gerespecteerd.

Waarschijnlijk zijn nog niet alle ambtenaren en professionals bekend met de privacyprotocollen. Bovendien zijn die van Samen DOEN en de OKT nog niet op internet geplaatst. Ook in het geval dat een ambtenaar of professional de afspraken uit deze set van ondersteunende documentatie één op één volgt, is de privacy niet geborgd. Het risico op bovenmatige gegevensverwerking is reëel aanwezig.

Geen zichtbare afweging proportionaliteit en subsidiariteit in het protocol
In de protocollen missen we aandacht voor een expliciete afweging of door de verwerking van de (bijzondere) persoonsgegevens de inbreuk op de belangen van de betrokkene onevenredig is ten opzichte van het doel (i.c. de hulpverlening) waarvoor de gegevens worden verwerkt (proportionaliteit). Ambtenaren en professionals worden niet aangemoedigd om deze afweging te maken. Dit geldt ook voor de afweging of het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene, minder nadelige wijze kunnen worden verwerkelijkt (subsidiariteit). Bij OKT wordt in de privacyworkshops wel aandacht besteed aan (de afweging van) proportionaliteit en subsidiariteit, door professionals een afwegingskader te bieden voor situaties waarin ze overwegen of ze gegevens moeten delen.

Protocol en instructies stimuleren een passende gegevensverwerking niet
Gegevens mogen alleen worden verwerkt voor zover dat voor een goede hulpverlening aan de betrokkene noodzakelijk is. Bij alle momenten waarop een afweging moet worden gemaakt over het verhelderen, routeren of escaleren van vragen en casussen moet ook worden afgewogen welke gegevens moeten worden vastgelegd en welke niet (meer). In de protocollen en werkwijzers ontbreekt de opdracht aan ambtenaren en professionals om deze afweging tijdens die triagemomenten te maken. Daarnaast worden gebruikers van RIS, Samen DOEN en Wijkzorg (voor ambulante zorg en dagbesteding), juist gestimuleerd om zo veel mogelijk persoonsgegevens van de betrokkene te weten te komen en vast te leggen. Deze gebruikers wordt aanbevolen om alle leefgebieden van de zelfredzaamheidsmatrix (ZRM) uit te vragen en te registreren. Dit om de situatie van de cliënt in beeld te kunnen brengen, maar bij Samen DOEN ook om de effectiviteit van het programma te kunnen monitoren. Met ZRM wordt informatie vastgelegd over bijvoorbeeld inkomen, dagbesteding, huisvesting, gezinsrelaties, geestelijke en fysieke gezondheid en verslavings- en justitieverleden. Overwegen professionals om bepaalde informatie niet te vragen of te registeren, dan wordt hen gevraagd deze keuze te motiveren.

Deze instructies worden in de praktijk als een verplichting opgevat. Bijna tweederde van de ambtenaren en professionals van Samen DOEN (64%) geeft aan niet zelf te mogen bepalen welke leefdomeinen zij invullen. Bij Wijkzorg geeft ongeveer de helft van de ambtenaren en professionals aan dat zij zelf bepalen mogen bepalen welke leefgebieden ze uitvragen en vastleggen.
Slechts de helft van de ambtenaren en professionals vinden dat er bij de ZRM geen sprake is van een voor de hulpverlening passende gegevensverwerking. Zij zijn van mening dat er precies genoeg informatie over de betrokkene wordt vastgelegd in de zelfredzaamheidsmatrix (ZRM) om hun taak te kunnen uitoefenen.

Door de gekozen formulering in het privacyprotocol kan bij ambtenaren en professionals de indruk ontstaan dat het is toegestaan, of zelfs verplicht is, om ook het burgerservicenummer (BSN) te registreren van anderen dan de hulpbehoevende betrokkene. Dit is echter niet toegestaan. Bij Wijkzorg is dit inmiddels verholpen door

RIS-Wijkzorg zo aan te passen, dat het BSN nummer niet meer kan worden ingevuld voor een andere persoon dan de betrokkene zelf. Ook Samen DOEN onderkent dat er sprake is van bovenmatige gegevensverwerking, en gaat hier in de leerlijn aandacht aan besteden.

De leden van ons burgerpanel hebben aangeven van welke gegevens zij het in verschillende situaties logisch vinden dat de gemeente of instellingen deze opvragen om hulp te kunnen verlenen. De persoonsgegevens waren ontleend aan de ZRM en de situaties gerelateerd aan de drie modules Samen DOEN, OKT en Wijkzorg. De panelleden kiezen bij de situaties gegevens die passen bij de werkwijzers. De heldere keuzes van de panelleden laten zien dat ook burgers sommige gegevens niet nodig vinden voor die hulpverlening.

Open en algemene normen laten ruimte bovenmatige gegevensverwerking
De Wbp en de privacyprotocollen kennen ruime doelstellingen en open en algemene normen, zoals bijvoorbeeld 'zorgvuldig', 'evenredig', 'verenigbaar', 'spoedeisend', 'rechtstreeks betrokken bij hulpvraag' en 'een belang dat zwaarder weegt dan de zwijgplicht'. De set van documentatie geeft ambtenaren en hulpverleners door deze open normen weinig richting bij de uitvoering van hun taak, waardoor de kans bestaat dat ze buiten de bandbreedte van de Wbp treden en bovenmatig gegevens verwerken.

9.4 Het merendeel van de ambtenaren en professionals geeft aan de privacy-afspraken na te leven, toch kan de privacy nog beter worden gewaarborgd

Is de ervaring van de 552 geënquêteerde ambtenaren en professionals zodanig dat kan worden gesteld dat de privacy van de bij de hulpverlening betrokken burger in de praktijk wordt gewaarborgd?

Het merendeel van deze ambtenaren en professionals informeert de betrokkene over het doel van de gegevensverwerking (79%), welke gegevens zullen worden gedeeld met anderen (93%),een groot deel geeft de betrokkene toestemming om het cliëntdossier in te zien (85%), en is van mening dat hun eigen kennis van privacyregelgeving goed op orde is (60%). Het was echter onze verwachting dat bijna altijd aan deze normen zou worden voldaanomdat de wettelijke uitzonderings-mogelijkheden zeer beperkt zijn.

De privacy van betrokkenen kan beter worden gewaarborgd wanneer de voorlichting wordt verbeterd en gegevensverwerking afhangt van het doel van de hulpverlening.

Voorlichting aan de betrokkene kan beter
Positief is dat een burger via meerdere kanalen informatie krijgt aangereikt. Toch kan de bij de hulpverlening betrokken burger beter worden geïnformeerd over de te doorlopen stappen bij de hulpverlening, de triagemomenten en de (privacy)rechten van de betrokkene. Dit kan eenvoudig door consequent een folder of een brief mee te geven of toe te sturen. Verder kan de inhoud van de websites, folders en brieven worden verbeterd door meer informatie te geven over het delen van gegevens, wie toegang hebben tot het dossier, geheimhoudingsplicht en de rechtsbescherming via de bestuurs- of civiele rechter. De gekozen vormen van voorlichting sluiten minder goed aan bij de groep van (licht) verstandelijk gehandicapten en de groep van mensen met zware psychische problemen. Voor hen zullen de gangbare wijze van informeren minder passend zijn.

Een aanzienlijk deel van de bij de hulpverlening betrokken burgers wordt door de hulpverlenende ambtenaar of professional niet geïnformeerd over zijn rechten, waaronder het recht op inzage, wijzigen of verwijderen van gegevens. Een kwart van de professionals en ambtenaren geeft aan de betrokkene (bijna) nooit daarover te informeren.

Het burgerpanel heeft de voorkeur dat de gemeente en de instellingen hen voorlicht door middel van een brief voorafgaand aan de eerste hulpverlening (70,1%) en via de website (63,6%). Minder populair is een folder (22,3%) en mondelinge voorlichting (22,5%).

9.5 Goede belangenafweging tussen privacy en hulpverlening nog ingewikkeld

Om een goede belangenafweging tussen privacy en hulpverlening te kunnen maken zijn wij van mening dat de randvoorwaarden op orde moeten zijn. Dit blijkt nog niet het geval. Uit de praktijk blijkt dat ambtenaren en professionals worstelen met belangenafwegingen, ook in het geval dat gegevens worden gedeeld zonder voorafgaande kennisgeving of toestemming van de betrokkenen.

Niet alle randvoorwaarden dragen bij aan een goede belangenafweging
Enigszins positief zijn ambtenaren en professionals over de mate van aandacht voor privacy door hun organisatie (65%) en over de inschatting dat collega's zorgvuldig omgaan met privacygevoelige gegevens (70%).

Over andere randvoorwaarden is men uitgesproken negatief. Minder dan de helft ervaart de privacyregelgeving niet als belemmerend (42%), slechts een derde is van mening dat de scholingsmogelijkheden op orde zijn, en ongeveer een kwart vindt RIS gebruiksvriendelijk en overzichtelijk (functionaliteit) en slechts 37% stelt dat in RIS alle gegevens voldoende veilig zijn beschermd (autorisatie). Daarnaast is een derde van mening dat ze in RIS te veel gegevens moeten invoeren (bovenmatige gegevens-verzameling) en slechts circa 22% is er zeker van dat de gegevens die door anderen zijn ingevuld betrouwbaar zijn. Gegeven deze ervaringen van ambtenaren en

professionals verwachten wij dat de randvoorwaarden nog niet van een dusdanig niveau zijn om ondersteunend te kunnen zijn aan de belangenafweging die zij maken.

Ook bij belangenafweging is nadere concretisering noodzakelijk
Wanneer ambtenaren en professionals 12 praktijksituaties krijgen voorgelegd over het delen van gegevens met anderen, zonder dat de betrokkene daarover vooraf wordt geïnformeerd en mee instemt, zien we een grote diversiteit aan reacties.

Is de veiligheid van het kind in het geding dan is er een grote eensgezindheid om gegevens te delen (81%). Het merendeel geeft aan dat gegevens niet mogen worden gedeeld alleen omdat dan de informatie-uitwisseling efficiënt kan verlopen (56%), de dienstverlening aan de cliënt kan worden verbeterd (59%) of omdat de cliënt de Nederlandse taal niet machtig zou zijn (66%).

Ambtenaren en professionals zijn verdeeld hoe te handelen in de acht andere praktijksituaties. Ze geven aan dit te laten afhangen van de specifieke situatie. Soms zien we een lichte voorkeur voor het niet delen van gegevens, bij mogelijke overlast voor de omgeving, wanneer cliënten een verstandelijke of geestelijke beperking hebben of wanneer er een informeel signaal komt dat iemand hulp nodig heeft. Loopt de cliënt gevaar dan valt er een lichte voorkeur te bespeuren voor het wel delen van gegevens zonder toestemming van de cliënt. Afhankelijk van de situatie kiezen sommige ambtenaren en professionals er voor om (bijzondere) persoonsgegevens juist niet te registreren of te delen, of buiten RIS om vast te leggen.

Het burgerpanel heeft dezelfde situaties voorgelegd gekregen. De panelleden vinden het acceptabel gegevens te delen in situaties gerelateerd aan veiligheid (zoals de veiligheid van het kind). Ook is het acceptabel om gegevens te delen bij zorggere-lateerd situaties, maar hangt het in deze situaties vaker af van de context (zoals zorgmijdend gedrag). Als het delen een praktische reden heeft dan mogen professional en ambtenaren gegevens niet delen (zoals efficiëntere informatie-uitwisseling).

Deze diversiteit in antwoorden vraagt om een verdere ondersteuning van de ambtenaren en professionals voor het maken van belangenafwegingen in deze en andersoortige situaties.

Bijlage 1 – Definities en afkortingen

Definities

Adequate gegevensverwerking: Ambtenaren, hulpverleners en professionals kunnen de hen opgedragen taak efficiënt en effectief uitvoeren met behulp van de verzamelde persoonsgegevens.

Audit trail (bron: encyclo.nl, Nederlandse encyclopedie): het spoor van basisgegeven naar veredeld eindgegeven en omgekeerd; spoor van controleerbare vastleggingen.

Basis beveiligingsniveau (bron: Tactische baseline Informatiebeveiliging):
Het geheel van maatregelen van beveiliging dat wordt bereikt door het implementeren en toepassen van de normen zoals geformuleerd in de Code voor Informatiebeveiliging, Business Continuïty Management en artikel 16 van de WBP en waaraan de NORA een nadere uitwerking geeft, onder meer door normen voor ICT-voorzieningen

Betrokkene: Degene op wie een persoonsgegeven betrekking heeft.

BIG (bron: VNG, augustus 2013): Baseline Informatiebeveiliging Gemeente. De BIG is bedoeld om de gemeenten op een vergelijkbare manier efficiënt te laten werken met informatiebeveiliging, een hulpmiddel te geven om aan alle eisen op het gebied van informatiebeveiliging te kunnen voldoen, de auditlast te verminderen en gemeenten een aantoonbaar betrouwbare partner te laten zijn.

Bijzondere persoonsgegevens: Bijzondere persoonsgegevens zijn gegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, als ook persoonsgegevens betreffende het lidmaatschap van een vakvereniging, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag.

'dat' en 'wat' informatie (bron: Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, november 2014): bij de scheiding van dat- en wat informatie gaat het erom in hoeverre het mogelijk is voor een medewerker om eerst inzicht te krijgen in 'dat-gegevens' om vervolgens pas te beslissen of het nodig is om ook toegang te krijgen tot de wat-gegevens. Hierbij staan 'dat-gegevens' voor gegevens die aangeven dàt er sprake is van een bepaalde voorziening, bijvoorbeeld een Wmo-voorziening, en 'wat-gegevens' voor gegevens die informatie geven wat er om welke voorziening het gaat, of de meer inhoudelijke informatie over en problematiek.

Escrowregeling (bron: Wikipedia): een overeenkomst tussen de maker van software, zijn klanten en een escrow-agent. De overeenkomst garandeert dat de klant in bepaalde gevallen kan beschikken over de laatste broncode van het softwarepakket waarvoor de overeenkomst gesloten is. Een eindgebruiker van software heeft veel belang bij het voortbestaan van de software aangezien de bedrijfsvoering van de gebruiker er sterk afhankelijk van kan zijn. Op het moment dat een leverancier niet meer kan leveren door bijvoorbeeld een faillissement, het stoppen met een product(lijn) of door het niet voldoen aan leveringsverplichtingen en er moet een aanpassing aan het pakket plaatsvinden, dan kan de eindgebruiker dat zelf niet (laten) doen. Daarvoor is de beschikking nodig over de broncode.

Gegevensverwerking: Omvat het gehele proces dat een gegeven doormaakt. Het start met het moment van verzamelen van gegevens waarna deze gegevens worden gebruikt en eventueel gedeeld. Het proces eindigt met het moment van vernietiging van gegevens.

Informatiebeveiliging en de bescherming van de privacy (bron: Ontwikkelplan PIB cluster sociaal gemeente Amsterdam): is het geheel van preventieve,
detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen de organisatie garanderen, met als doel de continuïteit van de informatie en de
informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken van:

- continuïteit / beschikbaarheid (voorkomen van uitval van systemen),
- integriteit / betrouwbaarheid (gegevens zijn juist, actueel en volledig)
- exclusiviteit / vertrouwelijkheid (onbevoegden kunnen geen kennis nemen van informatie die een organisatie onder zich heeft)
- privacybescherming van alle gegevens van zowel de burger als medewerkers (conform de Wet Bescherming Persoonsgegevens)
- controleerbaar voldoen aan wet- en regelgeving (compliance).

Persoonsgegeven: is elk gegeven over een geïdentificeerde of identificeerbare natuurlijke persoon

PIA (bron: Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, november 2014): een Privacy Impact Assessment legt de risico's bloot van projecten die te maken hebben met privacy, en draagt bij aan het vermijden of verminderen van deze privacy risico's. De PIA doet dit - in beginsel - door op gestructureerde wijze door de mogelijke (negatieve) gevolgen van het gebruik van persoonsgegevens voor de betrokken personen en organisaties in kaart te brengen en de risico's voor de betrokken personen en organisaties zo veel mogelijk te lokaliseren. Dit, zo mogelijk, aangevuld met aanbevelingen gericht op het verminderen van risico's.

Privacy: het recht van elke burger om voor zichzelf te bepalen welke informatie over hem of haar hoe, wanneer, met wie en in welke mate wordt gecommuniceerd en waarbij minimaal aan de vereisten van de Wet bescherming persoonsgegevens is voldaan.

Transformatie (bron: Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, november 2014): een nieuwe werkwijze binnen het sociaal domein met onder andere regie voor de burger, meer preventie, de inzet van wijkteams en een omslag van 'zorgen voor' naar 'zorgen dat'.

Transitie (bron: Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, november 2014): de overgang van taken van het rijk naar de gemeenten.

Triage (bron: Privacy Impact Assessment Gemeentelijke 3D informatiehuishouding, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, november 2014): het proces van verhelderen, routeren en escaleren van vragen en casussen. Door middel van triage bepaalt een ambtenaar of professional of er sprake is van een enkelvoudige of meervoudige vraag, dan wel complexe (multiprobleem) casuïstiek en welke mate van gegevensverwerking daarbij hoort. Bij een eenvoudige en enkelvoudige vraag is de gegevensverwerking beperkt terwijl er bij een complexere vraag wellicht meer partijen betrokken zijn en dus meer gegeven verwerkt (en eventueel uitgewisseld) worden.

Zorgmijdend gedrag (bron: Calamiteitenonderzoek Amsterdam, borgen van veiligheid in kwetsbare gezinnen, september 2015): Onder zorgmijdend gedrag verstaat Samenwerkend Toezicht Jeugd/sociaal domein het beperkt of niet accepteren van hulp, of alleen het accepteren van hulp op terreinen die het gezin als niet bedreigend ervaart.

Afkortingen

BI:	BasisInformatie
BIG:	Baseline Informatiebeveiliging Gemeenten
BRP:	Basisregistratie Personen
BSN:	Burgerservicenummer
CAT:	Cluster Advies Teams
CBP:	College Bescherming Persoonsgegevens
CISO:	Chief Information Security Officer
CPA:	Commissie Persoonsgegevens Amsterdam
DJZ:	Directie Juridische Zaken
IB'er:	Informatiebeveiliger
IV:	InformatieVoorziening
IVE Sociaal:	Informatievoorziening eenheid van het cluster Sociaal
IVE's:	Informatievoorzieningseenheden
JGZ:	Jeugdgezondsheidszorg
NCSC:	Nationaal Cyber Security Centrum
OKA:	Ouder- Kind Adviseur
OKT:	Ouder- en Kindteams
OWASP:	Open Web Application Security Project
PAT-team:	Project Advies Team
PGB:	Persoonsgebonden budget
PIA:	Privacy Impact Assessment
PIB:	Privacy en Informatie Beveiliger (ook wel privacy coördinator)
PPM:	Project Portfolio Management
RIS:	Registratie Informatie Systeem
RRP:	Regeling Risicovolle Projecten
Rve GGD:	Resultaat Verantwoordelijke Eenheid Gemeentelijke ` Gezondheidsdienst
Rve OJZ:	Resultaat Verantwoordelijke Eenheid Onderwijs, Jeugd en Zorg
Rve WPI:	Resultaat Verantwoordelijke Eenheid Werk, Participatie en Inkomen
SAT:	Stedelijk Advies Team
URA:	Uitgebreide RisicoAnalyse informatiebeveiliging en privacy
VNG:	Vereniging Nederlandse Gemeenten
VOG:	Verklaring Omtrent Gedrag
VRA:	Verkorte RisicoAnalyse informatiebeveiliging en privacy
Wbp:	Wet bescherming persoonsgegevens
WGBO:	Wet op de Geneeskundige BehandelingsOvereenkomst
Wmo:	Wet maatschappelijke ondersteuning
ZRM:	Zelfredzaamheidsmatrix

Bijlage 2 - Normenkader Wet bescherming persoonsgegevens (Wbp)

De onderstaande normen uit de Wet bescherming persoonsgegevens zijn afgeleid en overgenomen uit:

- https://cbpweb.nl/nl/over-privacy/wetten/wbp-naslag
- Ministerie van Justitie, Handleiding voor verwerkers van persoonsgegevens, april 2002

Het betreft een selectie op basis van de wettelijke bepalingen, de wetsgeschiedenis en de jurisprudentie.

Normen
(Bijzondere) persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld en verder worden verwerkt. Verwerking vindt plaats op een behoorlijke en zorgvuldige wijze en gegevens worden niet langer bewaard dan nodig voor het doel.
• Gegevensverwerking is behoorlijk, zorgvuldig en in overeenstemming met de wet. Dit betekent dat de betrokkenen van het bestaan van de verwerkingen kennis kunnen hebben en, wanneer van hen gegevens worden verkregen, daadwerkelijk en volledig worden ingelicht over de omstandigheden waaronder deze gegevens worden verkregen.
• Gegevensverwerking is alleen toegestaan als er sprake is van een uitdrukkelijk, gerechtvaardigd en welbepaald doel waarvoor de gegevens worden verzameld. [483] Dit doel dient al te zijn vastgesteld bij het verzamelen van gegevens en geldt verder dan ook voor alle onderdelen van verwerken van de gegevens, waaronder het bijwerken en het samenbrengen van persoonsgegevens. Deze doelomschrijving moet duidelijk zijn, niet zo vaag of ruim dat zij bijvoorbeeld tijdens het verzamelproces geen kader kan bieden waaraan getoetst kan worden of de gegevens nodig zijn voor dat doel of niet. [484] • Meer in het algemeen kan worden opgemerkt dat het verzamelen van gegevens over willekeurige burgers voor een doel dat mogelijk in de toekomst relevant zal zijn, in beginsel niet is toegestaan. [485] • De gegevensverwerking voldoet aan de beginselen van proportionaliteit en subsidiariteit. Het *proportionaliteitsbeginsel* houdt in dat de inbreuk op de belangen van de bij de verwerking van persoonsgegevens betrokkene niet onevenredig mag zijn in verhouding tot het met de verwerking te dienen doel. Ingevolge het *subsidiariteitsbeginsel* mag het doel waarvoor de persoonsgegevens worden verwerkt in redelijkheid niet op een andere, voor de bij de verwerking van persoonsgegevens betrokkene minder nadelige wijze kunnen worden verwerkelijkt. [486]

[483] *Kamerstukken II*, 1997-1998, 25 892, nr 3 (MvT),p. 78-79

[484] *Kamerstukken II*, 1997-1998, 25 892, nr 3 (MvT), blz. 79

[485] II, nr. 6, blz. 34

[486] *Kamerstukken II*, 1997-1998, 25 892, nr 3 (MvT),p. 80

Normen
• Uit artikel 9 Wbp volgt dat het doel waarvoor de gegevens zijn verkregen als uitgangspunt en toetsingskader dienen voor iedere vorm van (verdere) gegevensverwerking. Gegevens mogen niet worden verwerkt op een wijze die onverenigbaar is met die doeleinden. Gegevens mogen dus wel worden gebruikt voor andere doeleinden dan waarvoor zij zijn verzameld. Doch dit andere doel dient verenigbaar te zijn met het oorspronkelijke. [487] • De overheid mag persoonlijke gegevens van iemand niet zomaar gebruiken. [488] • De eis van verenigbaar gebruik brengt met zich mee dat persoonsgegevens kunnen worden gekoppeld wanneer ten minste aan de eis is voldaan dat de doeleinden waartoe de gegevens oorspronkelijk zijn verzameld, met elkaar verenigbaar zijn.
• Gegevens worden slechts verwerkt indien: • De betrokkene voor de verwerking zijn *ondubbelzinnige toestemming* heeft verleend. Deze grondslag geldt alleen als rechtsgeldige grondslag voor de verwerking van persoonsgegevens als deze vrijwillig kan worden gegeven. In het sociaal domein kan worden gesproken van een afhankelijkheidsrelatie, in deze context tussen betrokkene en de gemeente. Toestemming voor verwerking van persoonsgegevens kan in een afhankelijkheidsrelatie niet vrij worden gegeven en derhalve niet de grondslag zijn voor verwerking van persoonsgegevens.[489] Ook als de gemeente bij de uitvoering van publiekrechtelijke taken nadrukkelijk zou aangeven dat het weigeren van toestemming voor de gegevensverwerking geen gevolgen zal hebben voor het in aanmerking komen voor een door betrokkene gewenste voorziening, neemt dat de afhankelijkheid van de burger ten opzichte van de gemeente niet voldoende weg, alsdus het CBP. In deze context zijn de randvoorwaarden voor het verkrijgen van een vrije en daardoor rechtsgeldige toestemming voor de verwerking van persoonsgegevens niet aanwezig. Ook als de gemeente optreedt als de daadwerkelijke hulpverlener (als aanbieder of als regisseur) zal moeten worden bekeken of daarbij de randvoorwaarden voor het verkrijgen van een vrije en daardoor rechtsgeldige toestemming van de burger voor verwerking van persoonsgegevens door toestemming door de gemeente wel aanwezig zijn. De afhankelijkheidsrelatie tussen burger en gemeente zal ook in deze situaties aanwezig zijn. [490] • De gegevensverwerking noodzakelijk is om een *wettelijke verplichting* na te komen waaraan de verantwoordelijke onderworpen is. Indien persoonsgegevens worden verwerkt op grond van een wettelijke verplichting is het van belang dat zonder verwerking van de gegevens het uitvoeren van de wettelijke verplichting redelijkerwijs niet goed mogelijk zijn. Er moet een evident verband bestaan tussen de gegevensverwerking en de (uitvoering van de) wettelijke verplichting. Een wettelijke verplichting rechtvaardigt niet iedere gegevensverwerking. De verantwoordelijke mag ter uitvoering van de wettelijke verplichting bij voorbeeld niet meer of andere gegevens verwerken dan noodzakelijk is voor de uitvoering van de wettelijke verplichting. Gelet op de aard van de inbreuk op de privacy is een belangenafweging van geval tot

[487] MvT, II, nr. 3, blz. 79.

[488] http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbl6ah4zz

[489] Zie ook W. Boor en A.M. van de Laar, Toestemming in de WMO 2015, Gemeentestem 2015/80

[490] Zie Cbp, Advies privacytoets jeugddomein, 30 oktober 2014, p. 5

Normen
geval nodig. Daarbij dient onder meer gelet te worden op de aard van de in het geding zijnde taak en de aard van de betrokken gegevens. [491] • De gegevensverwerking noodzakelijk is voor de goede *vervulling van een publiekrechtelijke taak* door het betreffende bestuursorgaan dan wel het bestuursorgaan waaraan de gegevens worden verstrekt. [492] Als er geen gedetailleerde wettelijke regels bestaan voor deze taakuitoefening, dient bijzondere aandacht te worden besteed aan de vraag of wel sprake is van een rechtmatige taakuitoefening. Bij de beoordeling van de noodzaak van de betrokken verwerking zullen verder de beginselen van proportionaliteit en subsidiariteit een belangrijke rol spelen.[493]
• Het doel waarvoor de gegevens zijn verzameld en vervolgens worden verwerkt, is bepalend voor de hoeveelheid en de soort gegevens die onderwerp van verwerking vormen. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend[494] en niet bovenmatig te zijn[495]. Indien de verantwoordelijke een zo beperkt aantal gegevens verwerkt dat in redelijkheid niet kan worden gezegd dat hij daarmee, gelet op de doeleinde waarvoor hij de gegevens wenst te verwerken, een juist beeld van de betrokkene heeft, overtreedt hij het voorschrift dat de gegevens met het oog op het doel waarvoor ze worden verwerkt, toereikend dienen te zijn.
• Een nummer dat ter identificatie van een persoon bij wet is voorgeschreven, wordt bij de verwerking van persoonsgegevens slechts gebruikt ter uitvoering van de betreffende wet dan wel voor doeleinden bij de wet bepaald. [496] Voorbeelden zijn van zulke nummers zijn het Burgerservicenummer, het A-nummer in de BRP (voorheen GBA), BIG-nummer. • Achtergrond: Een persoonsidentificerend nummer is een gegeven waarmee een individuele natuurlijke persoon kan worden geïdentificeerd. Uit een oogpunt van bescherming van de persoonlijke levenssfeer werd het noodzakelijk geacht om aan het gebruik van dergelijke nummers beperkingen te stellen. Vast staat immers dat persoonsnummers de koppeling van verschillende bestanden aanzienlijk vergemakkelijken en daarmee een extra bedreiging voor de persoonlijke levenssfeer vormen. • Overheidsorganisaties en zorgaanbieders mogen het burgerservicenummer (BSN) gebruiken om hun taak uit te voeren. Maar dat mag alleen wanneer het BSN hierbij noodzakelijk is. Organisaties buiten de overheid mogen het BSN alleen gebruiken als dit in een specifieke wet is bepaald. En alleen voor het specifieke doel dat in de wet staat omschreven. [497]
• Mocht verdere verwerking inhouden dat de verantwoordelijke de gegevens aan derden verstrekt, dan zal hij in beginsel niet wederom verplicht zijn de betrokkene te informeren. In zoverre heeft de informatieverplichting een eenmalig karakter. [498] Dit is anders als er wijzigingen voordoen in de informatie. Bijvoorbeeld doordat de verantwoordelijke de gegevens aan andere personen

[491] (MvT, II, nr. 3, blz. 83)
[492] MvT, II, nr. 3, blz. 85
[493] Kamerstukken II, 1997-1998, 25 892, nr 3, blz. 84
[494] Kamerstukken II, 1997-1998, 25 892, nr 3, blz. 96-97
[495] Kamerstukken II, 1997-1998, 25 892, nr 3,, blz. 96
[496] Art 24 lid 1 Wbp
[497] https://cbpweb.nl/nl/onderwerpen/identificatie/burgerservicenummer-bsn?qa=bsn
[498] Kamerstukken II, 1997-1998, 25 892, nr 3,, blz. 157

Normen
wil verstrekken dan de categorieën ontvangers die hij de betrokkene heeft medegedeeld. Dan zal hij de betrokkene van deze wijziging op de hoogte moeten stellen. [499]
• Gegevens worden niet langer bewaard dan nodig is voor het doel, tenzij gegevens moeten worden gearchiveerd, bijzondere regels een langere bewaringstermijn
Degene van wie (bijzondere) persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze (bijzondere) persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.
• De betrokkene is vooraf geïnformeerd over de gegevensverwerking, in het geval dat de betrokkene gegevens zelf verstrekt.
• Een betrokkene moet in beginsel altijd op de hoogte zijn van het feit dat zijn gegevens worden verwerkt, door wie zijn gegevens worden verwerkt en voor welke doeleinden zijn gegevens worden verwerkt.[500] • De verantwoordelijke is verplicht om op eigen initiatief de betrokkene steeds op de hoogte te stellen van het bestaan van de gegevensverwerking, tenzij deze daarvan reeds op de hoogte is. De betrokkene heeft geen onderzoeksplicht. Beschikt de betrokkene over de informatie, bijvoorbeeld omdat deze hem is overhandigd of toegezonden, dan is hij daarmee op de hoogte, ongeacht of hij het initiatief heeft genomen de informatie ook tot zijn bewustzijn te brengen. [501]
• In het geval dat de gegevens buiten de betrokkenen om wordt verkregen moet de betrokkene uiterlijk op het moment dat de gegevens worden vastgelegd worden geïnformeerd. Zo ook bij bestandskoppeling. Tenzij het onmogelijk is om alle betrokken te informeren of als de gegevensverzameling op grond van een wettelijke plicht plaatsvindt.
• De betrokkene moeten tussentijds worden geïnformeerd als informatie aan derden zal worden verstrekt waarvan de betrokkene nog geen weet heeft.
• De informatie moet aan de betrokkene worden verstrekt op het moment van verzamelen. Gebeurt dit verzamelen via een formulier dan kan de informatie op het formulier worden voorgedrukt. Wanneer de betrokkene het formulier invult kan hij de informatie lezen. Het is dan niet nodig dat hij met zijn handtekening te kennen geeft ook deze informatie te hebben gelezen. Hetzelfde geldt voor de overhandiging van een folder of een exemplaar van standaardvoorwaarden bij het sluiten van een contract. Weigert de betrokkene de folder of het exemplaar aan te nemen, dan komt dit voor zijn rekening. De verantwoordelijke heeft dan aan zijn verplichtingen voldaan. Onvoldoende is dat op een formulier wordt verwezen naar elders verkrijgbare informatie. [502] • Indien de verantwoordelijke de betrokkene heeft geïnformeerd (op grond van artikel 33) zal hij de gegevens vervolgens kunnen verwerken. [503] • De informatieplicht is een belangrijk instrument om het gegevensverkeer transparant te maken. Hierdoor wordt de verantwoordelijke ook aanspreekbaar voor de betrokkene. Ook stelt het de betrokkene in staat om te volgen hoe

[499] II, nr. 3, blz.154

[500] De informatieverplichtingen uit de artikelen 33 en 34 van de Wbp gelden in alle gevallen zie verder. EK 34, blz. 34-1627

[501] MvT, II, nr. 3, blz. 149-151 en I, nr. 92c, blz. 3

[502] II, nr. 3, blz. 152

[503] II, nr. 3, blz. 157

Normen
gegevens over hem worden verwerkt en bepaalde vormen van verwerking of onrechtmatig gedrag van de verantwoordelijke in rechte aan te vechten. De omvang van de informatieplicht hangt af van wat nodig is om een "fair processing" te waarborgen. [504] • Gevolg van niet-informeren leidt tot onrechtmatige verwerkingen. Daarnaast kan het zijn, dat onder omstandigheden verdergaande informatie geboden is om "een eerlijke verwerking" te waarborgen. [505] • De informatieplicht geldt niet als de vastlegging of de verstrekking bij of krachtens de wet is voorgeschreven. In dat geval dient de verantwoordelijke de betrokkene op diens verzoek te informeren over het wettelijk voorschrift dat tot de vastlegging of verstrekking van de hem betreffende gegevens heeft geleid. [506] • Indien gegevens worden verkregen door koppeling van diverse bestanden, moet de verantwoordelijke de betrokkene informeren over de wijze waarop hij deze nieuwe gegevens heeft verkregen. Koppeling legt dan een extra verantwoordelijkheid bij de verantwoordelijke. De informatieplicht in het geval van koppelen omvat bijvoorbeeld de verplichting de betrokkene op de hoogte te stellen van het feit dat de gegevens zijn verkregen middels een koppeling van bestanden, een omschrijving van de soort bestanden die zijn gekoppeld en het wijzen van de betrokkene op zijn recht op toegang en verbetering van de gegevens. [507]
De verantwoordelijk zorgt er voor dat de betrokkene kan beschikken over haar gegevens en de mogelijkheid heeft om gegevens te verbeteren en verwijderen
• Iedereen heeft er recht op te zien wat er over hem is vastgelegd. En kan gegevens laten veranderen als ze niet juist zijn. [508] • De betrokkene heeft het recht zich vrijelijk en met redelijke tussenpozen tot de verantwoordelijke te wenden met het verzoek hem mede te delen of hem betreffende persoonsgegevens worden verwerkt. De verantwoordelijke deelt de betrokkene schriftelijk binnen vier weken mee of hem betreffende persoonsgegevens worden verwerkt. [509] Het mededelen kan ook elektronisch. [510] In het geval dat gegevens over hem worden verwerkt dan dient de verantwoordelijk een volledig overzicht ter beschikking stelt van de gegevens met inlichtingen over doel, de aard van de gegevens en van de ontvangers, alsmede over de herkomst van de gegevens. [511] • Indien de verzoeker minderjarig is (leeftijd < 16 jaar) of onder curatele is gesteld, wordt het verzoek gedaan door hun wettelijke vertegenwoordigers. [512] • Uitgangspunt is dat de informatie zodanig moet worden verstrekt dat de betrokkene daarover daadwerkelijk beschikt. In de praktijk kan dit op velerlei wijze. In een rechtstreeks individueel contact tussen (een vertegenwoordiger van) de verantwoordelijke en betrokkene kan de informatie mondeling of

[504] MvT, II, nr. 3, blz. 149-151 en I, nr. 92c, blz. 3
[505] MvT II, nr. 3, blz. 149-150
[506] Art 34 lid 5 Wbp
[507] II, nr. 3, blz. 154
[508] http://www.denederlandsegrondwet.nl/9353000/1/j9vvihlf299q0sr/vgrnbl6ah4zz
[509] Art 35 lid 1
[510] II, nr. 8, blz. 27
[511] II, nr. 3, blz. 158
[512] Art 37 lid 3

Normen
schriftelijk worden verstrekt. Ook kan de informatie in de vorm van data worden verstrekt. [513] • De verantwoordelijke moet de identiteit van de verzoeker vaststellen om te voorkomen dat iemand door het gebruik van de naam van een ander, gegevens over deze kan krijgen. [514] Een kopie van een identiteitsbewijs van betrokkene plus een eventuele schriftelijke machtiging is in beginsel een redelijke waarborg. Dit kan per post worden aangeboden of ter plaatste worden getoond. [515] • Op grond van artikel 36 kan de betrokkene correctie verzoeken indien de gegevens feitelijk onjuist, voor het doel van de verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijke voorschrift worden verwerkt. Het hoeft niet altijd te gaan om een de verantwoordelijke verwijtbare onrechtmatige gedraging. Indien bepaalde persoonsgegevens feitelijk onjuist zijn, heeft de betrokkene ook recht op verbetering zonder dat de verantwoordelijke tekort is geschoten in zijn zorgplicht voor de juistheid van die gegevens. De verantwoordelijke bericht de verzoeker binnen vier weken na ontvangst van het verzoek schriftelijk of dan wel in hoeverre hij daaraan voldoet. Een weigering is met redenen omkleed. [516] De Verantwoordelijke draagt zorg dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. [517] • Indien de gegevens zijn verbeterd, aangevuld, verwijderd of afgeschermd moet de verantwoordelijk dit zo spoedig mogelijk te melden aan derden waaraan al in een eerder stadium de gegevens waren verstrekt, tenzij dit onmogelijk blijkt of een onevenredige inspanning kost. [518] • Persoonsgegevens worden niet langer bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerkelijking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt. Dit brengt met zich dat de verantwoordelijke zich dient af te vragen of er redenen zijn op grond waarvan gegevens vastgelegd kunnen blijven. Zijn er voldoende redenen dan kan hij bepalen welke termijnen gelden om die gegevens te bewaren. • Zijn die termijnen verlopen dan zal hij de gegevens niet meer mogen verwerken, tenzij voor een ander, daarmee verenigbaar doel, bij voorbeeld statische archivering. [519] Soms mogen gegevens voor een onbepaalde tijd worden bewaard. In dit verband kan worden gewezen op de archiefbescheiden als bedoeld in de Archiefwet 1995 die naar een archiefbewaarplaats zijn overgebracht. Voor deze bescheiden geldt onder meer als doeleinde: behoud van (een deel van) het Nederlandse culturele erfgoed. Daarmee is de termijn gedurende welke de daarin opgenomen persoonsgegevens mogen worden bewaard, in beginsel onbepaald. [520] • Ook is soms in bijzondere wetgeving de algemene termijn gedurende welke de gegevens kunnen worden bewaard, gefixeerd.[521] Voorts kunnen in de algemene

[513] II, nr. 3 blz. 152
[514] II, nr. 3, blz. 161
[515] CBP 18 December 2002, z2002-01511
[516] Art 35 lid 2.
[517] Art 36 lid 3
[518] Art 38 lid 1
[519] MvT, II, nr. 3, blz. 95.
[520] MvT, II, nr. 3, blz. 96.
[521] MvT, II, nr. 3, blz. 95

Normen
maatregel van bestuur als bedoeld in artikel 29 - gelet op het tweede lid, onder e van dit artikel - criteria of termijnen worden geformuleerd.[522] En de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de desbetreffende gegevens uitsluitend voor deze specifieke doeleinden worden gebruikt. [523]
• Binnen vier weken moet de verantwoordelijke beslissen of de betrokkene inzage krijgt in zijn persoonsgegevens, nadat de identiteit van de verzoeker is vastgesteld.
• Betrokkene moet kunnen beschikken over de gegevens. In een rechtstreeks individueel contact tussen (een vertegenwoordiger van) de verantwoordelijke en betrokkene kan de informatie mondeling of schriftelijk worden verstrekt. Ook kan de informatie in de vorm van data worden verstrekt.
• De verantwoordelijke besluit binnen vier weken of persoonsgegevens worden verbeterd, aangevuld, verwijderd of afgeschermd.
De gegevensverwerking moeten op een passende manier worden beveiligd en geheimgehouden

• De verantwoordelijke zorgt voor passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Ook als deze verwerking plaatsvindt door een ander persoon die niet rechtstreeks is onderworpen aan zijn gezag (de bewerker). De verantwoordelijke ziet toe op de naleving hiervan. [524]
• Onder onrechtmatige vormen van verwerking vallen de aantasting van de gegevens, onbevoegde kennisneming, wijziging, of verstrekking daarvan. De beveiligingsverplichting strekt zich uit tot alle onderdelen van het proces van gegevensverwerking.
• Het begrip 'passende' houdt in dat:
  • de beveiliging in overeenstemming is met de stand van de techniek. Dit is in eerste aanleg een vraag van professionele ethiek van personen belast met de informatiebeveiliging.
  • de beveiligingsmaatregelen en de aard van de te beschermen gegevens proportioneel zijn. Naarmate bijvoorbeeld de gegevens een gevoeliger karakter hebben, of de context waarin deze worden gebruikt een grotere bedreiging voor de persoonlijke levenssfeer betekenen, worden zwaardere eisen gesteld aan de beveiliging van de gegevens. Er is geen verplichting om steeds de aller zwaarste beveiliging te nemen.
  • de maatregelen in overeenstemming dienen te zijn met de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico voor de persoonlijke levenssfeer van betrokkenen inhouden, dienen zwaardere eisen aan de beveiliging van de gegevens te worden gesteld
• Als de verantwoordelijke nalaat te zorgen voor een passend beveiligingsniveau, pleegt hij een onrechtmatige daad jegens de betrokkenen en kan daarvoor door deze aansprakelijk worden gesteld. Dit kan leiden tot veroordeling en

[522] MvT, II, nr. 3, blz. 95
[523] MvT, II, nr. 3, blz. 96.
[524] Art 13 Wbp

Normen
vergoeding van (im)materiele schade die de betrokkene heeft geleden. Daarnaast kan het College bestuursdwang toepassen.[525] • Het EHRM oordeelt dat het gebrek aan beveiliging van medische gegevens in een ziekenhuis een inbreuk is op artikel 8 EVRM. In het ziekenhuis was geen beperking van wie toegang had tot de medische dossiers en controle achteraf was moeilijk. [526]
• De geheimhoudingsplicht (art 12 lid 2) geldt voor de bewerker, alsmede degenen die onder het gezag van de verantwoordelijke of de bewerker werkzaam zijn. • In beginsel kan slechts een uitdrukkelijke wettelijke verplichting op de geheimhoudingsplicht een inbreuk maken. Daarnaast kan de geheimhouding worden doorbroken voor zover uit de taak van de betreffende persoon de noodzaak tot mededeling voortvloeit. Of een noodzaak tot mededeling aanwezig is, wordt bepaald door de verantwoordelijke onder wiens gezag of in wiens opdracht de persoon werkzaam is. Uiteraard is deze bevoegdheid van de verantwoordelijke evenmin onbegrensd. De verantwoordelijke is immers op zijn beurt gehouden aan regels inzake doelbinding en verenigbaar gebruik.

[525] MvA, I, nr. 92c, blz. 15-16

[526] EHRM 17 juli 2008, 20511/03

Bijlage 3 – Geraadpleegde functionarissen en documenten

Geraadpleegde functionarissen

- Francien Anker, Programmadirecteur OKT
- Marco van Beek, CISO a.i.
- Marleen Beumer, Externe Programmadirecteur OKT
- Gaston Bokhoven, beleidsmedewerker programma Om het Kind
- Yvette Bommeljé, onderzoeker en adviseur in het gemeentelijk domein
- Ben Booij, Projectmanager Wijkzorg
- Peter van Bosheide, projectleider Sociaal Domein
- Mirjam Buter, coördinator functioneel beheer RIS-modules
- Hermien Buyse, Adviseur Kwaliteit bij OKT met privacy als aandachtsgebied, Altra
- Laurens Conijn, (voormalig) Projectmanager Informatievoorziening (extern)
- Anne-Maartje Douqué, Ambtelijk Secretaris Commissie Persoonsgegevens Amsterdam
- Hayat Elbouk, Projectleider/Privacy coördinator Samen DOEN
- Arthur van der Endt, Functioneel Beheerder RIS, OKT
- Marijn Fraanje, Hoofd CIO-office
- Wilmar Hendriks, Dossierhouder Privacy Jeugdhulp
- David van Hooff, Senior Audit Manager
- Ticho van Hoppe, Accountmanager Inforing
- Ron Huisen, Beleidsmedewerker Jeugd
- Arjan de Jager, Strategisch informatiemanager, Informatievoorziening Sociaal
- Oktay Kaya, Portfoliomanager, CIO-office
- Enno van Kessel, Functioneel beheerder RIS-OKT en RIS-SD
- Marguerite Koenigs, voormalig Beleidsadviseur en juriste bij Cluster Sociaal
- Jacko van der Meulen, Programmamanager Samen DOEN
- Jaap de Munnik, Beleidsadviseur Informatiebeveiliging en Privacy, CIO-office
- Benny Norbart, Senior Applicatiebeheerder (o.a RIS-JG)
- Christine Pollmann, Afdelingshoofd Jeugd
- Luuc Posthumus, voormalig Voorzitter Commissie Persoonsgegevens Amsterdam
- Robert Jan Prenger, Programmamanager Informatievoorziening Jeugddomein
- Prof. Mr. Dr. W.L. Roozendaal, bijzonder hoogleraar Sociale zekerheidsrecht, Faculteit der Rechtsgeleerdheid Vrije Universiteit Amsterdam
- Patrick Snoek, Procesmanager Zorg voor de Jeugd
- Ward Stadhouders, Business Controller Samen DOEN
- Suzette Spoelstra, Beleidsadviseur rve BI

- Robert Jan Taling, Coördinator Privacy, Informatiebeveiliging en Bedrijfscontinuïteit (PIB) Cluster Sociaal
- Wigger Tenge, teamleider Activeringsteam 2, Stadsdeel Zuid
- Gaby van Uitert, generalist en aandacht functionaris privacy Samen DOEN
- Rob Ulrich, Beleidsadviseur Informatiebeveiliging en Privacy CIO-office
- Theo Veltman, manager IV Sociaal
- Karin Walters, Teammanager FB team 2
- Cees Wiering, Beleidsadviseur Informatievoorziening CIO-office
- Elleke Wolf, Informatiemanager

Geraadpleegde documenten

- Stedelijk directeur sociaal, feitelijk wederhoor, 17-2-2016
- Individuele escrow-overeenkomst voor broncode inzake RIS-modules, Gemeente Amsterdam, 12 februari 2016
- College B en W, Bestuurlijke reactie Commissie Persoonsgegevens Amsterdam jaarverslag 2014, 18 januari 2016
- Protocol Richtlijn voor beveiligd mailen met en tussen jeugdhulpverlener, Gemeente Amsterdam, 18 januari 2016
- ACAM, Rapport privacycontrol 1ste en 2de lijn, 16 februari 2016
- Brief Inwerkingtreding meldplicht datalekken per 1 januari 2016, 17 december 2015
- Inview, Adviesrapport RIS Wijkzorg 2nd opinion. Een perspectief voor de korte termijn, 27 november 2015
- Memo beveiliging RIS , 16 november 2015
- Plan van aanpak, bevindingen n.a.v. hack- en pentest en her-test, 4 november 2015
- Privacyprotocol Samen DOEN in de buurt, oktober 2015
- Brief cliënt persoonlijke gegevens Wijkzorg, oktober 2015
- RIS Wijkzorg: gebruikers handleiding, versie oktober 2015
- Calamiteitenonderzoek Amsterdam - Borgen van veiligheid in kwetsbare gezinnen, september 2015.
- Privacyprotocol OKT, september 2015
- Privacyprotocol Wijkzorg, september 2015
- Rapport Nulmeting Privacyschouw Jeugd Amsterdam, september 2015
- Eerste tussentijdse rapportage fase Nulmeting "Privacyschouw Jeugd Amsterdam", 17 augustus 2015
- Stand van zaken en ervaringen met Wijkzorg, commissie flap raadscommissie voor Zorg en Welzijn en Sport en Recreatie, 25 juni 2015
- Implementatieplan Baseline Informatiebeveiliging Gemeenten (BIG), versie 2, 25 juni 2015
- Campagne Bewustwording Informatiebeveiliging & Privacy 2015/2016, 14 juni 2015
- Staf Flap, Agendapunt, 18 mei 2015
- Rekenkamer Amsterdam, onderzoeksopzet privacy voor burgers, 29 april 2015
- Samen DOEN in de buurt: Handleiding Registratieproces in RIS versie 2, april 2015
- Hoofdovereenkomst tussen Gemeente Amsterdam en de leverancier, versie 1.2, 9 maart 2015
- Bewerkersovereenkomst tussen Gemeente Amsterdam en de leverancier, bijlage van de Hoofdovereenkomst, 9 maart 2015
- Gemeente Amsterdam, Releasenote RIS-Wijkzorg versie 2.4, februari 2016

- “Wat doet u met mijn gegevens?” Zorg voor de privacy, versie februari 2015
- Stedelijk kader Wijkzorg, versie januari 2015
- Uniforme Werkwijze Samen DOEN in de buurt, versie januari 2015
- W. Boor en A.M. van de Laar, Toestemming in de WMO 2015, Gemeentestem 2015/80
- Meldformulier incident privacy, 2015
- PrivacyCare, 'Privacy Impact Assessment in verband met gegevensverwerking bij de uitvoering van de Jeugdwet door gemeenten' (rapport in opdracht van de Directie Justitieel Jeugdbeleid), gepubliceerd als bijlage bij Kamerstukken I 2014/15, 33 684, Q
- Afwegingskader, versie 2014
- VNG, Handreiking communiceren met burgers over privacy, december 2014
- Raadsbrief *Contractering Wmo 2015*, 8 december 2014
- Transparantiedocument SD versie 1.1, 28 november 2014
- Transparantiedocument OHK versie 1.0, 28 november 2014
- Raamovereenkomst in het kader van Wmo 2015 Ambulante ondersteuning, Dagbesteding & Kortdurend verblijf, november 2014
- Bewerkersovereenkomst in het kader van Wmo 2015 Ambulante ondersteuning, Dagbesteding & Kortdurend verblijf, november 2014
- De Zelfredzaamheid-Matrix (ZRM), versie november 2014
- Factsheet Privacy, november 2014
- Rapport Privacy Impact Assessment Gemeentelijke 3D Informatiehuishouding, Rijksoverheid, november 2014
- Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014
- Addendum Privacy 2015/RIS (bijlage van Samenwerkingsovereenkomst Ouder- en Kindteams Amsterdam, 23 oktober 2014)
- Samenwerkingsovereenkomst Samen DOEN, oktober 2014
- Gebundelde krachten: Evaluatie Samen DOEN in de buurt in Amsterdam, oktober 2014
- Voortgangsrapportage risicomanagement sociaal domein: Voortgang en risico’s van de decentralisaties Jeugdwet, AWBZ/Wmo, Participatiewet, de samenhang tussen de drie decentralisaties (3D), Samen DOEN en Dragende samenleving, oktober 2014
- Verkorte Risicoanalyse Informatiebeveiliging en Privacy, versie 1.5, 8 september 2014
- Transparantiedocument JG versie 1.0, 29 augustus 2014
- Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy; Cluster sociaal IV systeem RIS 3D’s, versie 1.2, 28 augustus 2014
- Privacy Impact Assessment: RIS modules Om het Kind, Samen DOEN en Wijkzorg, 20 augustus 2014

- Richtsnoer beveiliging webapplicaties gemeente Amsterdam; Beleidskader en methodiek voor het beoordelen van de beveiliging van nieuwe en bestaande webapplicaties, versie 1.0, 15 mei 2014
- Beleidsvisie 'Zorgvuldig en Bewust; gegevensverwerking en privacy in een gedecentraliseerd sociaal domein', Rijksoverheid, 1 mei 2014
- Stadsbrede IV-kaders, De basis voor de Amsterdamse informatiehuishouding, CIO Office, 10 maart 2014 Versie 1.1
- College van B en W, Notitie *'Toekomst van de wijkteams in Amsterdam'*, 2014
- Jaarverslag 2014; Commissie Persoonsgegevens Amsterdam, 2014
- Uitgebreide Risicoanalyse Informatiebeveiliging en Privacy, versie 1.2, 4 december 2013
- Privacy Impact Analyse: Toelichting, versie 0.1, 6 november 2013
- Brief opdrachtformulering Juridische ondersteuning 3 D's, 22 oktober 2013
- Handleiding Registratieproces in RIS, Samen DOEN, 14 oktober 2013
- Visie op leren en ontwikkelen: De Samen DOEN in de buurt leerlijn, juli 2013
- Visie op leren en ontwikkelen: De Samen DOEN in de buurt leerlijn, juli 2013
- Koersbesluit Om het Kind, 15 mei 2013
- Programmaplan II (2013 – 2014) Om het Kind, 19 maart 2013
- Gemeente Amsterdam, Auditketen (controletoren), 7 oktober 2012
- Notitie 'Taken, verantwoordelijkheden en werkafspraken inzake het gemeentelijk gebruik van persoonsgegevens', november 2011
- Notitie 'Nut en noodzaak Commissie Persoonsgegevens Amsterdam', 15 september 2011
- Samenwerken in de Jeugdketen, een instrument voor gegevensuitwisseling, ministerie van VWS, versie 1.0 voorjaar 2011
- Herziening gemeentelijk beleid voor het gebruik van persoonsgegevens, 27 augustus 2009
- Ministerie van Justitie, Handleiding voor verwerkers van persoonsgegevens, april 2002
- Koops en Vedder, Opsporing versus privacy, Universiteit van Tilburg, 2001
- Kamerstukken II, 1997-1998, 25 892, nr 3(MvT)
- Klachtenregeling Gemeente Amsterdam, <geen datum>
- Privacy Q&A op de werkwijze OKT, OKT Amsterdam, <geen datum>
- Toestemmingsformulier uitwisselen gegevens Samen DOEN, <geen datum>
- Toestemmingsformulier opvragen zorggegevens OKT, <geen datum>
- Gemeente Amsterdam, Spreadsheet RIS OKT techniekissues, <geen datum>
- Janssen, L., De Kleine Gids, Privacy en beroepsgeheim in het sociale domein 2015, 2015

Websites

- https://www.amsterdam.nl/gemeente/organisatie/ruimte-economie/wonen/gemeente-privacy/
- https://www.amsterdam.nl/veelgevraagd/?productid=%7B249D3A8E-ED07-4E4C-BFAD-49F174342FD5%7D
- https://www.amsterdam.nl/zorg-welzijn/programma-samen-0/samen-west/
- https://www.amsterdam.nl/gemeente/organisatie/sociaal/onderwijs-jeugd-zorg/zorg-wmo-beleid/wegwijs-wmo/nieuws-wegwijs-wmo/2014/wijkzorg-privacy/
- https://www.amsterdam.nl/zorg-welzijn/programma-samen-0/samen/
- https://www.amsterdam.nl/gemeente/organisatie/sociaal/onderwijs-jeugd-zorg/zorg-wmo-beleid/wegwijs-wmo/nieuws-wegwijs-wmo/2014/wijkzorg-privacy/
- https://www.amsterdam.nl/zorg-welzijn/zorg-ouderen/wijkzorg/
- https://www.amsterdam.nl/gemeente/organisatie/sociaal/onderwijs-jeugd-zorg/wegwijs-in-de-wmo/wmo-docs-voorziening/wijkzorg/
- http://intranet.amsterdam.nl/kennis-beleid/algemeen/klachtencoordinatie/klachtbehandeling/
- http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/iv-management/
- http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/project-portfolio/ppm-inhetkort/
- http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/project-portfolio/ppm-proces/komt-cio-oordeel/
- http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/project-portfolio/ppm-proces/komt-cio-oordeel/
- http://intranet.amsterdam.nl/kennis-beleid/bedrijfsvoering/informatie/project-portfolio/ppm-proces/komt-cio-oordeel/
- http://www.ggd.amsterdam.nl/jeugd-0/jgz-privacy/
- http://www.oktamsterdam.nl/

Bijlage 4 – Enquête onder (oud) RIS-gebruikers

Voor het onderzoek is er in de maanden oktober en november 2015 een enquête verspreid naar professionals in het sociaal domein. Een belangrijk instrument bij de gegevens verwerking is het Registratie Informatie Systeem (RIS). Door middel van deze enquête willen we inzicht krijgen in hoe de gebruikers RIS gebruiken en beoordelen en hoe ze bij gegevensverwerking met persoonsgegevens en privacy omgaan.

De enquête is primair gericht naar professional en ambtenaren die werkzaamheden uitvoeren met RIS. Hierbij is een onderscheid gemaakt tussen de RIS-modules Samen DOEN, OKT, Wijkzorg en Jeugd en gezin. Ook zitten er professional en ambtenaren tussen die gebruik maken van andere RIS-modules en respondenten die geen gebruik maken van RIS. Aan deze respondenten zijn alleen algemene vragen gesteld.

De geanonimiseerde data en resultaten van de enquête kunnen in overleg en onder voorwaarden door de rekenkamer ter beschikking worden gesteld voor nader onderzoek.

Vragenlijst
Deze vragenlijst bestond uit meerkeuzevragen en open vragen. Ook zijn enkele feitelijke gegevens gevraagd over de achtergrond van de respondenten. Als een respondent met meerdere RIS-modules werkt moest aangegeven worden voor welke RIS-module de vragenlijst is ingevuld.

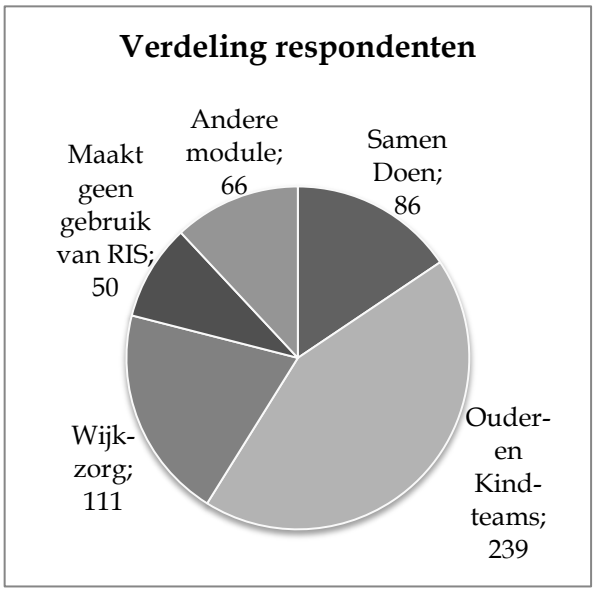
De vragenlijst bestond uit de volgende onderdelen:
- Raadplegen van documenten;
- Informeren van en toestemming vragen aan cliënten;
- Invoeren en bewerken van gegevens;
- Zelfredzaamheidsmatrix;
- Delen van gegevens met andere professionals;
- De mogelijkheid voor cliënten om gegevens in huns dossier in te zien;
- De mogelijkheid voor cliënten om gegevens te laten wijzigen en verwijderen;
- Situaties die de uitvoering van uw werkzaamheden kunnen bevorderen of juist belemmeren;
- Omgang met privacygevoelige gegevens binnen het sociaal domein;
- Situaties waarin gegevens gedeeld zouden kunnen worden.

Verspreiding van enquête
De enquête is verspreid in samenwerking met de dienst Onderzoek, Informatie en Statistiek (OIS) van de gemeente Amsterdam en de verantwoordelijke voor RIS binnen de gemeente Amsterdam. OIS heeft de vragenlijst gedigitaliseerd, de vragenlijst rondgestuurd en de data beheert. De verantwoordelijke van RIS heeft in

overleg ons toestemming gegeven de emailadressen van de RIS-gebruikers op te vragen bij de leverancier.

Eind oktober heeft OIS een digitale vragen rondgestuurd naar de professionals van de desbetreffende RIS-modules. De professionals en ambtenaren hadden 2,5 week de tijd de enquête in te vullen. In de tussentijd is nog een herinneringsmail gestuurd om de respons te vergroten. Uit de eerste resultaten bleek de respons van de Samen DOEN-respondenten laag. Om deze reden zijn de professionals en ambtenaren van Samen DOEN nogmaals verzocht de enquête in te vullen.

Respons (verdeling casegroepen)
In totaal hebben 552 professionals en ambtenaren deelgenomen aan het onderzoek (zie figuur). Vanwege de inrichting van het onderzoek en de lage respons is gekozen de respondenten van Jeugd en Gezin buiten het onderzoek te houden.
De overgebleven drie RIS-modules waar we specifiek analyse naar doen leveren samen 436 respondenten. OKT heeft met 239 respondenten het grootste aandeel in de respons. Zij worden gevolgd door Wijkzorg met 111 respondenten. Van Samen DOEN hebben 86 professionals de enquête ingevuld. Voor de verlenging hadden 56 respondenten van Samen DOEN de enquête ingevuld.



Naast de respondenten van de onderzochte RIS-modules hebben 66 respondenten deelgenomen aan het onderzoek die een andere RIS-module gebruiken voor gegevensregistratie. Een derde van deze respondenten zijn van Jeugd en Gezin.

Bijlage 5 - Verslag Groepsgesprek Samen DOEN

Inleiding
De Rekenkamer Metropool Amsterdam voert momenteel onderzoek uit naar privacybescherming en gegevensverwerking in het sociale domein in de gemeente Amsterdam. Onderdeel van het onderzoek is een verdieping van het thema bij een uitvoerende partij: Samen DOEN. 23 november 2015 is een Versnellingskamer, een groepsbijeenkomst, georganiseerd waaraan vier teamleiders en zes teamleden (generalisten) van Samen DOEN hebben deelgenomen. De deelnemers hebben aan de hand van vragen en stellingen gediscussieerd over privacyaspecten in de dagelijkse werkpraktijk. In dit verslag worden de ervaringen en opmerkingen van de deelnemers beschreven. In het algemeen kan worden opgemerkt dat er weinig verschillen zijn tussen de opmerkingen van teamleiders en teamleden.

Ervaringen met privacybescherming en gegevensverwerking

Privacykader
Het privacykader biedt een heldere richtlijn over wat kan en mag in het registreren en delen van privacygevoelige informatie van cliënten. Hetzelfde geldt voor de regelgeving in het algemeen. Teamleden gebruiken voornamelijk het privacyprotocol en de uniforme werkwijze als informatiebronnen. Teamleiders gebruiken soms ook nog de Wbp, de meldcode huiselijk geweld (die bijvoorbeeld een handreiking biedt over illegaliteit, wat nog niet in protocollen is vastgelegd) en kindermishandeling en de samenwerkingsovereenkomst als informatiebronnen. De meeste deelnemers vinden de regels duidelijk en overwegend eenduidig. Er is voldoende informatie, en als men het even niet weet, dan kan men terugvallen op collega's of leidinggevenden. Dit gebeurt regelmatig. Eén deelnemer vindt dat er meer aandacht moet komen voor de regels voor het delen van medische gegevens.

Maar uitsluitend bekendheid met de regels is niet altijd toereikend voor een goede toepassing ervan in de praktijk. Het kader zelf mag dan duidelijk zijn, het is desondanks soms lastig om in de praktijk met het privacykader te werken. Dat komt omdat verschillende andere partijen (politie, GGZ, etc.) met andere kaders werken, maar ook vanwege de complexe situaties in de praktijk en ten slotte omdat je niet overal vertrouwelijke gesprekken kunt voeren vanwege de locatie waar gewerkt wordt. Het privacykader verhindert soms dat kan worden 'doorgepakt', bijvoorbeeld als men overlastgegevens met een straatcoach zou willen delen, of in situaties waarin al eerder meldingen zijn geweest of toestemming is gegeven. Veiligheid is een geldige reden om af te wijken van het protocol maar er zijn verschillende interpretaties van situaties waarin veiligheid al dan niet in het geding is. De definitie van crisis of 'uitzondering' is niet voor iedereen hetzelfde. Dit vraagt om maatwerk en onderling overleg.

Privacybewustzijn
Het is belangrijk om cliënten goed te informeren over privacy, daar is iedereen het over eens. Het helpt bij een goede samenwerking tussen professional en cliënt, maar daarentegen is het de vraag of iedere cliënt het ook begrijpt, want het komt voor dat dit in de praktijk tot problemen leidt. De deelnemers vinden dit een groot knelpunt, wat niet wegneemt dat hulpverleners privacy op alle niveaus moeten kunnen uitleggen. Ze zeggen dat ze over het geheel genomen wel een goed idee hebben van wat ze aan gegevens mogen vragen en delen, maar dat het – als het om de details gaat – soms wat zoeken is. In die gevallen wordt er pragmatisch gehandeld: het wordt openlijk en integer met de cliënt gesproken, ook omdat die werkwijze belangrijk is voor het succes van de zorgverlening zelf. Teamleden gebruiken daarnaast het eigen team altijd als aanvullende input wenselijk is, bij onduidelijke regels of vraagstukken die lastig op te lossen zijn. Sommigen bespreken een casus het liefste openlijk (met de namen), anderen hebben geen bezwaar tegen het anoniem bespreken van casussen. Men vindt dat het al dan niet anoniem bespreken van casussen binnen het team in ieder geval een bewuste keuze moet zijn. Het belang van de cliënt is een belangrijke reden om van de privacyregels af te wijken. Het gaat dan met name om situaties waarin de veiligheid van personen en kinderen in het geding is. Maar ook wanneer het in belang van de samenleving is, wordt wel eens afgeweken van de regels. Hier wordt opgemerkt dat je niet per se van de regels hoeft 'af te wijken', omdat het een plicht is melding te doen van onveilige situaties voor cliënten en samenleving.

Informeren en toestemming vragen van cliënt bij het registreren en delen van gegevens
Het vragen om toestemming van cliënten om gegevens te registreren is nodig omdat professionals op die manier aanvullende expertise kunnen inschakelen (in de eerste plaats van het team). Andere argumenten die zijn genoemd: verantwoording afleggen en transparantie richting de cliënt. Enkele professionals noemen de volgende redenen om cliënten (eventueel) niet om toestemming te vragen gegevens te registreren: vanwege de veiligheid van gezinsleden, omdat het vanzelfsprekend noodzakelijk is voor het verkrijgen van hulpverlening of omdat cliënten het mogelijk niet begrijpen. Als cliënten geen toestemming geven dan is dat voor een deel van de professionals geen reden om de zorg te stoppen. Zij zeggen dat het afhankelijk is van de situatie. Soms is wat meer tijd nodig om uit te leggen waar Samen DOEN voor is. De ene deelnemer zegt dat zonder toestemming niet kan worden begonnen met hulp en de andere zegt dat nergens staat dat je dan niet mag helpen. Er is een dilemma tussen de verantwoordelijkheid van de hulpverlener en de grenzen van de gegevensbescherming. De zorgverlening door Samen DOEN is vrijwillig, dus cliënten hoeven niet per se zorgverlening te accepteren. Maar de gemeenten heeft een zorgplicht, dus voor de professionals geldt soms juist wel een verplichting van melding of registratie.

Recht op inzage cliënt
Cliënten mogen volgens de professionals in principe altijd hun eigen gegevens inzien. Uitzonderingen zijn er wel: bijvoorbeeld als er sprake is van gescheiden ouders en de een de gegevens van de ander zou kunnen inzien. Of als gegevens oneigenlijk zouden kunnen worden gebruikt in een rechtszaak. Daarbij komt dat in de praktijk de 'eenheid' in een dossier niet altijd het gezin is en wie dan de cliënt is, is soms onduidelijk. Er zijn gesplitste dossiers omdat er regelmatig meer gezinnen op hetzelfde adres wonen. Er kunnen daarnaast in principe twee dossiers worden aangelegd in het geval van een echtscheiding, hoewel dit niet wenselijk is.

Invoeren en bewerken van gegevens
Er is geen kenmerkende situatie waarin professionals om meer gegevens vragen dan vanuit de eigen taak is toegestaan. Professionals mogen naar alle leefgebieden (bij de Zelfredzaamheidsmatrix) van de cliënten vragen. Professionals geven aan de meeste noodzakelijke gegevens ook te kunnen vragen, als dat maar op een respectvolle manier gebeurt. Gegevens over medicatie en psychiatrische gegevens zijn uitzonderingen. Een enkeling geeft aan dat niet per se alle informatie die wordt gevraagd, hoeft te worden geregistreerd. Op deze manier is de gewenste informatie wel bekend maar wordt deze niet opgeslagen.

Delen van gegevens: specifieke situaties en dilemma's
Gegevensdeling gebeurt volgens de meerderheid van de deelnemers ook op andere manieren dan met RIS. Dat gebeurt om het traject soepel en snel te laten verlopen, omdat het ook mondeling kan, omdat het om nieuwe aanmeldingen gaat, of omdat andere partijen geen gebruik maken van deze RIS-module. Veel hulpverleners sturen cliënten inmiddels een cc wanneer gegevens met andere partijen worden gedeeld via een e-mail, zegt een deelnemer. Een deel van de teamleden vindt het delen van gegevens met andere professionals niet goed geregeld. De teamleiders vinden allemaal dat dit wel goed geregeld is. Een minderheid van de deelnemers vindt het lastig om gegevens te delen vanwege de verschillende beroepscodes. Een groter deel van de teamleiders dan van de teamleden vindt dat niet zorgvuldig met privacy-gevoelige gegevens wordt omgegaan in de eigen organisatie. Het gaat dan om het mailen tussen collega's onderling, waarbij cliënten met naam en toenaam worden genoemd. De meeste deelnemers vinden daarentegen wel dat privacygevoelige gegevens alleen aan andere professionals wordt verstrekt als dat volgens de regels mag.

In specifieke situaties deelt men soms gegevens met andere partijen, zonder directe toestemming van cliënten. Er zijn geen duidelijke gemeenschappelijke kenmerken van specifieke situaties, het is volgens de meeste professionals echt afhankelijk van de situatie zelf, of het nodig of wenselijk is om gegevens te delen. Het is dus altijd maatwerk. Dit draagt volgens sommige deelnemers wel het risico met zich mee dat de grens tussen privacy en veiligheid kan verschuiven. Het wordt in ieder geval belangrijk gevonden dat hulpverleners zich kunnen verantwoorden over de keuze om het belang van veiligheid te laten prevaleren boven privacy.

- Zorgmijdend gedrag: gegevens worden met name gedeeld als de veiligheid van cliënten of hun omgeving in het geding is of bij gezondheidsrisico's.
- Vermoeden van fraude: professionals vinden dat de verantwoordelijkheid soms bij het huishouden moet worden gelegd, dus in eerste instantie moet worden besproken met het huishouden zelf. Het is afhankelijk van het soort en de ernst van de fraude of dit wordt gemeld, ook wordt de teamleider om advies gevraagd.
- Vermoeden van criminaliteit: het hangt af van de soort en de ernst van de criminaliteit en het wordt gerelateerd aan de specifieke zorgvraag en de gevolgen van de melding voor het hele gezin. Wat hier verder een rol kan spelen is de eigen veiligheid van de professional, meer nog dan de gevolgen voor de samenleving. Het zou dus kunnen voorkomen dat iemand geen melding maakt terwijl dit wel verplicht kan zijn (als er sprake is van strafbare feiten). Ook hier worden dergelijke situaties vaak aan de teamleider voorgelegd. Eén deelnemer voelt zich hierin ook voldoende gesteund door de gemeente. Er is een voldoende vangnet voor hulpverleners.
- Efficiënte informatie-uitwisseling: hier is geen eensluidende omschrijving gegeven, wel wordt opgemerkt dat het niet de bedoeling is, maar dat het soms wel om die reden zal gebeuren.
- Gezondheidsrisico's: dit soort situaties lijken vrij duidelijk. Als er sprake is van direct gevaar, voor de cliënt of zijn omgeving (infectieziekten) dan worden gegevens gedeeld.
- Betere dienstverlening aan cliënten: wordt over het algemeen niet als een geldige reden gezien om gegevens te delen. Er zijn wel situaties denkbaar waarin het wenselijk is om het traject te versnellen (denk aan wachttijden). Dit wordt dan met de cliënt besproken.
- Veiligheid van cliënten: dit is zeker een situatie waarin gegevens worden gedeeld, zeker als het om kinderen gaat.
- Cliënten die niet de Nederlandse taal machtig zijn: is vrijwel nooit een geldige reden om af te wijken van het protocol. Professionals geven aan dat dan een tolk moet worden ingeschakeld.
- De cliënt heeft een verstandelijke of geestelijke beperking: bij deze groep cliënten kan het wel eens voorkomen dat gegevens zonder toestemming worden gedeeld.
- Er is een informatiesignaal dat iemand mogelijk hulp nodig heeft: afhankelijk van het signaal. Eén deelnemer zegt dat degene die het signaal heeft opgevangen dan moet handelen.
- Overlast voor de omgeving: afhankelijk van de aard en de ernst van de overlast.

Er worden nog andere dilemma's genoemd in privacybescherming enerzijds en het goed kunnen uitoefenen van taken anderzijds: het gaat dan om de culturele achtergrond van de cliënt, bij gevoelens van schaamte (niet verder toegelicht), bij een verhuizing naar een andere stad of over de wijze waarop je een plan van aanpak opschrijft. Dilemma's komen ook voor bij cliënten die mogelijk pedofiel zijn, of bij uitbehandelde tbs'ers, bij vermoedens van radicalisering of bij oud-cliënten (als ze bijvoorbeeld een vuurwapen dragen).

Rekenkamer Amsterdam

Postbus 202
1000 AE Amsterdam

telefoon 020 25 478 08
info@rekenkamer.amsterdam.nl
www.rekenkamer.amsterdam.nl