unravelling
ONDERZOEK & ADVIES

Rekenkameronderzoek
Privacy in het sociaal domein

Rekenkamer BEL
6 februari 2017

Onderzoekers:
- Martijn Mussche
- Laura Meijer

Samenvatting

Normen	Score	Bevinding
Beleid voor de borging van privacy		
De BEL-gemeenten hebben de uitgangspunten voor het privacybeleid beschreven en vastgesteld	De gemeenten voldoen	De drie BEL-gemeenten hebben ieder het Privacyprotocol Sociaal Domein HBEL (privacyprotocol) vastgesteld met daarin de uitgangspunten van het privacybeleid. Daarnaast kent de BEL Combinatie een Handboek Informatiebeveiliging en een ambtseed.
De BEL-gemeenten (dan wel de uitvoerende gemeente[1]) hebben de risico's voor het beheer, gebruik en de uitwisseling van persoonsgegevens (voor de drie decentralisaties) onderzocht.	De gemeenten voldoen niet	De BEL-gemeenten leunen sterk op de kennis en kunde van de gemeente Huizen en de Regio Gooi en Vechtstreek. Deze hebben voorafgaand aan het opstellen van het privacyprotocol onderzoek gedaan, maar er is geen indicatie dat er een specifieke risico-analyse is uitgevoerd.
De BEL-gemeenten (dan wel de uitvoerende gemeente) hebben normen voor het beheer, het gebruik en de uitwisseling van persoonsgegevens door medewerkers van de gemeente en andere betrokken partijen.	De gemeenten voldoen deels	De normen voor het beheer, het gebruik en de uitwisseling van persoonsgegevens door medewerkers van de gemeenten zijn verwerkt in het Handboek Informatiebeveiliging en het privacyprotocol sociaal domein. Echter het beheer, het gebruik en de uitwisseling van persoonsgegevens door andere betrokken partijen worden niet expliciet gemaakt in het privacyprotocol. In het privacyprotocol is de volgende zinsnede opgenomen: “Welke informatie zij (andere partijen) mogen verstrekken wordt bepaald door de privacywetgeving waaronder de betreffende partij valt en hun eigen privacyregelingen.”
Wet bescherming persoonsgegevens		
De richtlijnen en beleidsregels voldoen aan de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens (samengevat): a) Persoonsgegevens mogen alleen op een zorgvuldige manier worden verwerkt. b) Persoonsgegevens mogen alleen voor bepaalde, vooraf omschreven en gerechtvaardigde doeleinden worden verzameld… c) Degene van wie persoonsgegevens worden verwerkt, moet op de hoogte zijn van de identiteit van de organisatie die deze persoonsgegevens verwerkt en van het doel van de gegevensverwerking. d) De gegevensverwerking moeten op een passende manier worden beveiligd...	De gemeenten voldoen	Het privacyprotocol sociaal domein HBEL geeft uitvoering aan subnormen b en c. De beveiliging van de persoonsgegevens komt tot uiting in het Handboek Informatiebeveiliging, waardoor de gemeenten ook aan subnorm d voldoet. Subnorm a is overkoepelend en abstracter van aard is te beschouwen als gedachtegoed waarmee de richtlijnen en beleidsregels zijn geschreven. Daarmee voldoen de gemeenten aan de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens.

[1] De uitvoerende gemeente is de gemeente die de betreffende (deel)taak in het sociaal domein uitvoert in opdracht van de gemeente Blaricum, Eemnes en/of Laren. Het kan gaan om Huizen (als centrumgemeente in HBEL-verband), om Amersfoort of om Eemnes (jeugdzorg voor Eemnes).

Normen	Score	Bevinding
Toezicht op privacyborging		
De BEL-gemeenten en de uitvoerende gemeente hebben afspraken gemaakt over de bescherming van gegevens, bijvoorbeeld over werkvoorschriften, procedures en protocollen voor het gebruiken, uitwisselen en bewaren van persoonsgegevens.	De gemeenten voldoen deels	De documenten op basis waarvan de samenwerking met Huizen en Amersfoort zijn ingericht spreken niet over afspraken omtrent de bescherming van gegevens, anders dan de bepaling in de overeenkomst met Amersfoort dat Amersfoort zich moet houden aan relevante wet- en regelgeving waaronder de Wbp en Wet brp. Er wordt gewerkt vanuit het uitgangspunt dat overheden elkaar kunnen vertrouwen. Specifieke afspraken over werkvoorschriften, procedures en protocollen voor het gebruik, uitwisselen en bewaren van persoonsgegevens zijn onderdeel van het Privacyprotocol Sociaal Domein HBEL, dat door de vier samenwerkende gemeenten vastgesteld is. In de DVO met Amersfoort is opgenomen dat de gemeente Amersfoort zich moet houden aan de bij die gemeente geldende richtlijnen.
De BEL-gemeenten houden toezicht op de juridische borging van privacy.	De gemeenten voldoen niet	Er zijn geen afspraken gemaakt over het toezicht op de naleving van deze afspraken. Daarnaast richten noch de BEL-gemeenten, noch de BEL Combinatie het toezicht op eigen initiatief in.
Communicatie met inwoners		
De BEL-gemeenten hebben een passend protocol voor het communiceren over de omgang met persoonsgegevens.	De gemeenten voldoen	De gemeente Huizen maakt op verschillende manieren inzichtelijk waarom gegevens verwerkt worden en welke mogelijkheden inwoners daarbij hebben. Het privacyprotocol is vindbaar op de website van de uitvoeringsorganisatie. Ook bij de toestemmingsverklaring is een bijlage met dezelfde informatie. Het Jeugd- en Gezinsteam Eemnes heeft dezelfde informatie en een link naar het privacyprotocol op zijn website. In geval van calamiteiten is er in Huizen en in Amersfoort oog voor privacy van de inwoners van de BEL-gemeenten. Met deze verschillende informatiekanalen voldoen de BEL-gemeenten aan de norm.
Informatie-uitwisseling met ketenpartners		
De afspraken rond informatie-uitwisseling met ketenpartners zijn duidelijk en passend.	De gemeenten voldoen deels	De bevinding over de afspraken met ketenpartners is vooral gebaseerd op de gesprekken met de betrokken gemeenten. De samenwerking met ketenpartners in het sociaal domein kent al een lange historie; afspraken rond informatieuitwisseling zijn niet nieuw, maar de decentralisaties zorgen voor meer uitwisseling van privacygevoelige gegevens. Ketenpartners hanteren daarbij hun eigen privacyreglementen.
BEL-gemeente, uitvoerende gemeente en ketenpartners zijn op de hoogte van de afspraken en handelen ernaar.	De gemeenten en ketenpartners voldoen deels	Uit gesprekken blijkt echter dat waar de aandacht en zorg voor privacyborging bij de gemeenten toeneemt, dit nog niet altijd het geval is bij ketenpartners. Er zijn meerdere voorbeelden waarbij ketenpartners – overigens met de beste intenties- soepeler zijn met het delen van informatie dan de uitvoerende gemeente passend acht.
Risico's		
De uitvoerende gemeente rapporteert aan de BEL-gemeenten over de diverse typen risico's rond informatiebeveiliging en privacy.	De gemeenten voldoen niet	Privacy is een maar één van vele belangrijke aspecten in het sociaal domein; er is geen specifieke managementinformatie over. De uitvoerende gemeente rapporteert niet apart aan de BEL-gemeenten over de diverse typen risico's rond informatiebeveiliging en privacy.
De BEL-gemeente is zich bewust van de risico's; dit is te zien in beheersmaatregelen.	De gemeenten voldoen deels	De uitvoerende gemeenten Huizen en Eemnes/Amersfoort zijn zich bewust van de risico's; dit is te zien in beheersmaatregelen. De BEL Combinatie staat op afstand en is niet rechtstreeks betrokken of aangehaakt bij beheersmaatregelen.

Aanbevelingen

De Rekenkamer BEL komt tot de volgende aanbevelingen:

Aan de gemeenteraden:

1. De aanbeveling van de Rekenkamer BEL uit 2015 over de uitvoering van een *GAP*- en risicoanalyse met betrekking tot digitale veiligheid is nog steeds actueel. [2] Vraag het college om de CISO de *GAP*- en risicoanalyse te laten uitvoeren en laat u informeren over de uitkomst.
2. Vraag het college om managementinformatie over de risico's rond privacy en informatiebeveiliging.

Aan de colleges van B en W:

3. Stimuleer het 'veilig' melden van datalekken. Zorg voor registratie van voorvallen en bijna-voorvallen met betrekking tot privacy, met uitsluitend als doel om daarvan te leren en te verbeteren. Medewerkers moeten te allen tijde incidenten kunnen melden zonder risico op persoonlijke consequenties.
4. Breid het beveiligd mailen uit tot alle relevante ketenpartners in het sociaal domein. Evalueer de toepassing van het beveiligd mailen en betrek daarbij zowel de ervaring van de gemeenten als van de ketenpartners.
5. Onderzoek de werking en toepassing van het privacyprotocol in de praktijk. Breng in kaart waar de gemeentelijke uitvoeringsorganisatie knelpunten ervaart.
6. Onderzoek in hoeverre er verschillen zijn tussen de privacyreglementen van ketenpartners en het privacyprotocol van de BEL-gemeenten. Breng in kaart waar de ketenpartners knelpunten ervaren. Leg vast dat ook voor ketenpartners het privacyprotocol van de BEL-gemeenten als richtlijn geldt.

[2] Rekenkamer BEL, BEL op weg naar BIG, Digitale veiligheid BEL-gemeenten, Quick Scan, augustus 2015.

Inhoud

Afkortingen en begrippen

AP:	Autoriteit persoonsgevens (voorheen bekend als College Bescherming Persoonsgegevens)
BEL:	Blaricum, Eemnes en Laren
BIG:	Baseline Informatiebeveiliging Nederlandse Gemeenten
CISO:	Chief information security officer. Hoofd informatiebeveiliging binnen de gemeente.
DVO:	Dienstverleningsovereenkomst
FG:	Functionaris voor gegevensbescherming. Een interne toezichthouder op de verwerking van persoonsgegevens binnen de gemeente. Voor de BEL Combinatie geeft de CISO invulling aan deze taak, maar is niet formeel daarvoor aangewezen of geregistreerd.
GAP-analyse:	Analyse van de verschillen tussen de werkelijke en de gewenste situatie (norm)
HBEL:	Huizen, Blaricum, Eemnes en Laren
SoZa HBEL:	De gemeenschappelijke regeling tussen de HBEL-gemeenten op het vlak van het sociaal domein
Wbp:	Wet bescherming persoonsgegevens
Wmo:	Wet maatschappelijke ondersteuning

1. Inleiding

1.1 Introductie

De samenleving wordt steeds complexer en door de decentralisaties zijn de laatste jaren steeds meer overheidstaken onder de verantwoordelijkheid van gemeenten komen te vallen. Gemeenten zijn sinds januari 2015 verantwoordelijk voor jeugdzorg, maatschappelijke ondersteuning en arbeidsparticipatie. Daardoor moeten gemeenten meer gegevens over burgers verzamelen en delen met andere partijen. Het gaat over naam-, adres- en woonplaatsgegevens, maar ook over de hulpvraag, de lichamelijke en geestelijke gezondheid, het strafrechtelijke verleden en werk- en inkomensgegevens. De verdergaande digitalisering van de samenleving maakt het delen van gegevens steeds makkelijker, maar ook meer en meer kwetsbaar. De aandacht bij gemeenten voor de bescherming van de privacy van burgers moet groot zijn. Een goede bescherming van persoonsgegevens draagt bij aan het vertrouwen van burgers in de gemeenten. In elk van de drie BEL-gemeenten is het college van burgemeester en wethouders verantwoordelijk voor de juridische borging van privacy. Het is daarmee aan de colleges om de privacyborging goed te organiseren en erop toe te zien dat de uitvoering conform wet- en regelgeving is.

De Rekenkamer BEL heeft medio 2016 besloten het onderwerp privacyborging in het sociaal domein door middel van een zogeheten korte toets te onderzoeken. In het jaarplan 2016 is het onderwerp juridische kwaliteitszorg opgenomen. Vanuit diverse fracties was een voorkeur uitgesproken voor een onderzoek op dat vlak. Na vooronderzoek heeft de Rekenkamer BEL besloten in eerste instantie te focussen op juridische borging van privacy in het sociaal domein.

1.2 Hoofdvraag, onderzoeksvragen en normenkader

De Rekenkamer BEL heeft de volgende hoofdvraag geformuleerd:

Hoe is in het licht van de toegenomen decentralisatie en verdergaande digitalisering de privacy van burgers juridisch geborgd binnen de gemeenten Blaricum, Eemnes en Laren en op welke punten behoeft dit verbetering?

Concreet laat zich dit vertalen in de volgende vragen en de daarbij behorende normen:

Onderzoeksvragen	Normen
1. Welke richtlijnen en beleidsregels hanteren de gemeenten van de BEL Combinatie voor de juridische borging van privacy?	▪ De BEL-gemeenten hebben de uitgangspunten voor het privacybeleid beschreven en vastgesteld. ▪ De BEL-gemeenten (dan wel de uitvoerende gemeente[3]) hebben de risico's voor het beheer, gebruik en de uitwisseling van persoonsgegevens (voor de drie decentralisaties) onderzocht. ▪ De BEL-gemeenten (dan wel de uitvoerende gemeente) hebben normen voor het beheer, het gebruik en de uitwisseling van persoonsgegevens door medewerkers van de gemeente en andere betrokken partijen.

[3] De uitvoerende gemeente is de gemeente die de betreffende (deel)taak in het sociaal domein uitvoert in opdracht van de gemeente Blaricum, Eemnes en/of Laren. Het kan gaan om Huizen (als centrumgemeente in HBEL-verband), om Amersfoort of om Eemnes (jeugdzorg voor Eemnes).

Onderzoeksvragen	Normen
2. Voldoen deze richtlijnen en beleidsregels aan de bepalingen uit de Wet bescherming persoonsgegevens?	▪ De richtlijnen en beleidsregels voldoen aan de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens:[4] a) Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt. b) Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn. c) Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking. d) De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.
3. Hoe zien de BEL-gemeenten erop toe dat de juridische borging van de privacy van een voldoende niveau is en blijft?	▪ De BEL-gemeenten en de uitvoerende gemeente hebben afspraken gemaakt over de bescherming van gegevens, bijvoorbeeld over werkvoorschriften, procedures en protocollen voor het gebruiken, uitwisselen en bewaren van persoonsgegevens. ▪ De BEL-gemeenten houden toezicht op de juridische borging van privacy.
4. Hoe communiceren de BEL-gemeenten naar burgers over de wijze waarop zij omgaan met persoonsgegevens?	▪ De BEL-gemeenten hebben een passend protocol voor het communiceren over de omgang met persoonsgegevens.
5. Hoe gaan de BEL-gemeenten om met privacygevoelige gegevens in het sociaal domein, mede gelet op de informatie-uitwisseling met ketenpartners?	▪ De afspraken rond informatie-uitwisseling met ketenpartners zijn duidelijk en passend. ▪ BEL-gemeente, uitvoerende gemeente en ketenpartners zijn op de hoogte van de afspraken en handelen ernaar.

[4] De gemeenten dienen te voldoen aan alle bepalingen in de Wbp. Voor dit korte onderzoek operationaliseren we dit in de vier belangrijkste bepalingen zoals de Autoriteit Persoonsgegevens die zelf aanduidt.

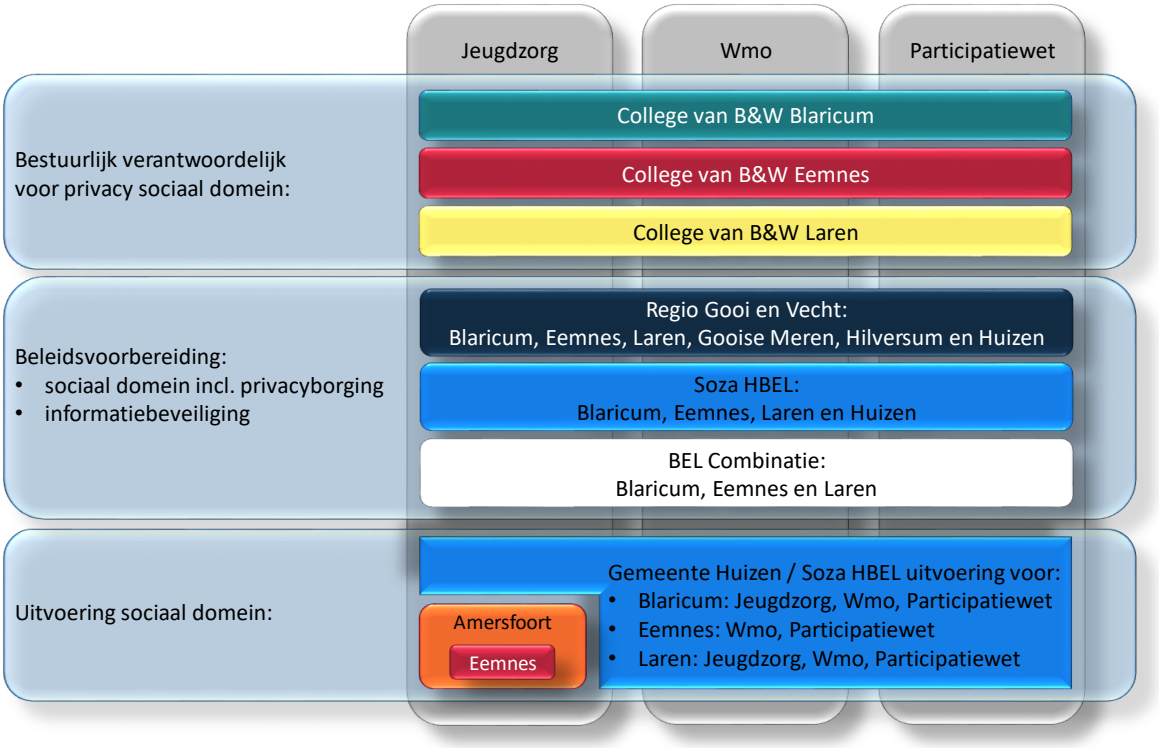
Onderzoeksvragen	Normen
6. Welke risico's zijn te onderkennen in de huidige wijze waarop de privacy van burgers juridisch geborgd is binnen de BEL-gemeenten?	▪ De uitvoerende gemeente rapporteert aan de BEL-gemeenten over de diverse typen risico's rond informatiebeveiliging en privacy[5]: a) Sociaal inhoudelijk, bijv. de dienstverlening komt niet op het gewenste niveau; b) Samenwerking, bijv. de afstemming met ketenpartijen en concernpartijen is onvoldoende; c) Juridisch, bijv. de privacy is onvoldoende geborgd in de manier waarop de systemen zijn ingericht en hulpverleners krijgen privégegevens onder ogen; d) Personeel, bijv. betrokken medewerkers implementeren de gewenste planning & controle maatregelen onvoldoende; e) Informatisering, bijv. de ICT-voorziening voldoet niet aan de gewenste kwaliteit. f) Organisatie en leiderschap, bijv. de sturing schiet te kort. g) Politiek, bijv. in hoeverre kan de raad casus inhoudelijk en op detailniveau bespreken; h) Economie/financieel, bijv. budgetoverschrijdingen doordat de ICT meer kost dan voorzien. ▪ De BEL-gemeente is zich bewust van de risico's; dit is te zien in beheersmaatregelen.

[5] Zie ook: Handreiking Financiën en de 3 decentralisaties, Ministerie van BZK, 14 februari 2014.

1.3 Afbakening en onderzoeksmethodiek

Dit rekenkameronderzoek is ingestoken als een zogeheten 'korte toets'.[6] Dit betekent dat de Rekenkamer BEL in kort tijdsbestek en met relatief geringe inzet van onderzoekscapaciteit een bondig antwoord wil krijgen op één hoofd-onderzoeksvraag.

De onderzoeksvragen zijn na het startgesprek met de ambtelijke directie op 29 augustus 2016 op een aantal onderdelen aangepast. Dit vanwege het feit dat de uitvoering van het sociaal domein deels in HBEL-verband en deels in Amersfoort plaatsvindt (zie de onderstaande figuur).



Figuur 1. Schematische weergave privacyborging in het sociaal domein in Blaricum, Eemnes en Laren

Uit de figuur is af te lezen dat er een gelaagd geheel is, doordat meerdere gemeenten en gemeentelijke samenwerkingen betrokken zijn bij de privacyborging in de drie BEL-gemeenten. Elke organisatie is met een kleur weergegeven. De drie colleges zijn bestuurlijk verantwoordelijk. De beleidsvoorbereiding vindt plaats op regionaal en op HBEL-niveau en de informatiebeveiliging is op BEL-niveau geregeld, in de gemeenschappelijke regeling SoZa HBEL. De operationele borging van privacy voor de drie BEL-gemeenten vindt plaats in Huizen, in Eemnes en in Amersfoort.[7] Binnen SoZa HBEL is onder aansturing van Huizen een intergemeentelijke afdeling Maatschappelijke Zaken ingericht, dit is de uitvoeringsorganisatie voor het sociaal domein voor de BEL Combinatie, met uitzondering van jeugdzorg van Eemnes. De Rekenkamer BEL heeft ervoor gekozen de focus in het rekenkameronderzoek vooral te leggen op het beleid en op de afspraken die de BEL-gemeenten hebben gemaakt over en toezicht op de uitvoering door derden. De uitvoering in de praktijk is daarmee niet onderzocht.[8]

[6] Zie ook het Onderzoeksprotocol van de Rekenkamer BEL.
[7] Huizen: Wmo en participatiewet voor de drie BEL-gemeenten, jeugdzorg voor Blaricum en Laren. Eemnes: jeugdzorg voor Eemnes. Amersfoort: administratieve verwerking voor jeugdzorg Eemnes.
[8] In de Startnotitie voor dit onderzoek stond nog de norm "De uitvoerende gemeente handelt conform het protocol".

De rekenkamer heeft voor dit onderzoek de relevante beleidsdocumenten, protocollen en overeenkomsten opgevraagd en bestudeerd. Vervolgens zijn gesprekken gevoerd met de verantwoordelijk manager (van de gemeente Huizen) en met medewerkers die betrokken zijn bij de beleidsvoorbereiding. Afgezien van jeugdzorg Eemnes, is niet gesproken met operationeel betrokkenen. De lijst met geraadpleegde personen is opgenomen in bijlage 1.

1.4 Leeswijzer

De onderzoeksvragen komen achtereenvolgens aan bod in de paragrafen 2.1 tot en met 2.6 van dit rapport. Elke paragraaf start met de onderzoeksvraag en gaat vervolgens in op de beantwoording van de betreffende onderzoeksvraag. De paragraaf wordt afgesloten met een oordeel over de mate waarin de gemeenten voldoen aan de – per onderzoeksvraag- gestelde normen. Hoofdstuk 3 bevat ten slotte de conclusies en aanbevelingen.

2. Bevindingen

2.1 Beleid voor de borging van privacy

Deze paragraaf gaat in op de volgende onderzoeksvraag:
Welke richtlijnen en beleidsregels hanteren de gemeenten van de BEL Combinatie voor de juridische borging van privacy?

Relevante beleidstukken rond privacy
De BEL Combinatie heeft een Handboek Informatiebeveiliging. Dit handboek heeft een vertrouwelijke status om eventuele kwaadwillenden geen inzicht te geven in de gemeentelijke informatiebeveiliging. Keerzijde is dat de toegankelijkheid van dit document daarmee beperkt is: burgers kunnen niet verifiëren of de gemeente zich aan zijn eigen handboek houdt. De Rekenkamer BEL heeft dit handboek op 14 september 2016 ingezien. Het is een beleidsstuk dat de reikwijdte heeft van de gehele BEL Combinatie, inclusief de in- en uitgaande informatiestromen tussen de BEL Combinatie en andere externe organisaties of personen. Het bevat zowel beleidsuitgangspunten als protocollen en procedures. Een landelijk uitgangspunt is dat overheden binnen Nederland elkaar kunnen vertrouwen, ook de BEL Combinatie noemt dat specifiek in haar handboek. Onderdeel van dit handboek is ook een procedure over de melding en afhandeling van incidenten, vallend onder de supervisie van de Chief Information Security Officer (CISO) van de BEL Combinatie. De CISO maakt jaarlijks een geheim jaarverslag met onder andere het aantal gemelde incidenten en bijna-incidenten en de maatregelen die hierop genomen zijn. Dit jaarverslag is bestemd voor de burgemeesters[9] en colleges van B&W en het Dagelijks Bestuur van de BEL Combinatie. De rekenkamer heeft het meest recente jaarverslag op 14 september 2016 ingezien en kan daarmee bevestigen dat dit verantwoordingsdocument over informatiebeveiliging bestaat. Vanwege het vertrouwelijke karakter kan de Rekenkamer BEL geen mededelingen op detailniveau doen over de inhoud van het document. Het sociaal domein is nog geen apart onderdeel van dit jaarverslag over de informatiebeveiliging.

Binnen de BEL Combinatie is er ook een Beleidsplan Informatie en ICT van juni 2016 dat zich richt op de informatiebeveiliging binnen de BEL Combinatie. De implementering van dit beleidsplan bevindt zich in een vroege fase. Door een tekort aan capaciteit zijn sommige ambities van dit beleidsplan nog niet in praktijk gebracht, zoals de uitvoering van een GAP-analyse. Dit zijn constateringen die de Rekenkamer BEL in 2015 ook al deed; deze zijn nog steeds actueel.[10]

Ambtseed
Naast bovenstaande beleidsstukken kent de BEL Combinatie een ambtseed. Een borging van privacy is in de ambtseed verweven door de frase ‘ik zal vertrouwelijk omgaan met (…) vertrouwelijke informatie’. De ambtseed is in werking getreden op 18 oktober 2013 en verplicht voor zowel de huidige ambtenaren als de nieuwe ambtenaren. Tijdelijk ingehuurde externe

[9] De burgemeester in dit geval als apart bestuursorgaan, naast het college van B&W.
[10] Rekenkamer BEL, BEL op weg naar BIG, Digitale veiligheid BEL-gemeenten, Quick Scan, augustus 2015.

medewerkers leggen geen ambtseed af, maar moeten een geheimhoudingsverklaring ondertekenen.

Totstandkoming van het privacyprotocol

Specifiek voor het sociaal domein bestaat er het Privacyprotocol Sociaal Domein HBEL (privacyprotocol). Dit privacyprotocol is vastgesteld door de colleges van Huizen (21 mei 2015), Blaricum (12 mei 2015), Eemnes (6 mei 2015) en Laren (12 mei 2015) en is daarmee het leidende protocol voor de uitvoering in deze gemeenten.

Het privacyprotocol is een product van regionale samenwerking. Vanuit het Uitvoeringsprogramma Sociaal Domein 2015-2016 van de Regio Gooi & Vechtstreek is een projectgroep 'Regie en Privacy Sociaal Domein' opgericht, waar medewerkers van de gemeenten Huizen, Hilversum en Bussum samen met medewerkers van de Regio werken aan een informatie- en handelingsprotocol privacy. De beleidsmedewerkers van de BEL Combinatie zijn overigens niet rechtstreeks betrokken geweest bij de totstandkoming van dit protocol, dat erop gericht is dat alle partijen in het sociaal domein voldoen aan alle privacyeisen en privacyvraagstukken. Daarnaast heeft de projectgroep een regierol voor privacy in het sociaal domein voor de deelnemende gemeenten, zorgaanbieders en cliënten. De deelnemende gemeenten zijn naast Blaricum, Eemnes, Laren en Huizen ook Hilversum Wijdemeren (voorheen Nederhorst den Berg, Ankeveen, 's-Graveland, Kortenhoef, Loosdrecht, en Breukeleveen), Weesp en Gooise Meren (voorheen Bussum, Naarden en Muiden).[11]

De ontwikkeling van het privacyprotocol is ook getriggerd door een rekenkameronderzoek naar schuldhulpverlening in Huizen. Een van de conclusies was dat er geen protocol gericht op privacy aanwezig was. Door een motie heeft de gemeenteraad van Huizen op 19 maart 2015 het college opgeroepen een protocol gericht op privacy in het totale sociaal domein op te stellen. Op 20 april 2015 heeft de afdeling Maatschappelijke Zaken HBEL het privacyprotocol voor vaststelling aan het college van Huizen gepresenteerd; het is op 21 mei 2015 vastgesteld door het college van Huizen. In het collegevoorstel staat beschreven dat het privacyprotocol afgestemd is met de BEL-gemeenten.[12] De colleges van de BEL-gemeenten hebben ieder ook in mei 2015 het protocol vastgesteld.

Inhoud van het privacyprotocol

Het privacyprotocol bestrijkt de verwerking van persoonsgegevens binnen het sociaal domein zoals uitgevoerd door de gemeenschappelijke regeling SoZa HBEL (HBEL). Het betreft de ontvangst en verwerking van gegevens door derden aan HBEL en de verzending van gegevens door HBEL aan derden, maar het betreft niet de afwegingen en procedures van derden. Het protocol is volledig gericht op HBEL en de medewerkers van HBEL. Het richt zich op de omgang van persoonsgegevens, de toestemming voor het delen van informatie, het delen van informatie zonder toestemming, het recht van betrokkene om inzage te hebben in de informatie en de wettelijke regelingen rondom bewaartermijnen en vernietiging van gegevens. De belangrijkste punten van het protocol volgen uit de Wet bescherming persoonsgegevens (Wbp). Het betreft de volgende drie principes:

[11] Met ingang van 1 januari 2016 zijn Bussum, Naarden en Muiden gefuseerd en gaan zij verder als de gemeente Gooise Meren.
[12] Gemeente Huizen, Collegevoorstel van 22 april 2015 voor het college van B&W van Huizen om kennis te nemen van en in te stemmen met het Privacyprotocol Sociaal Domein HBEL. Op 21 mei 2015 besloot het college conform dit voorstel.

1. De verwerking van persoonsgegevens moet passen binnen het doel waarvoor deze verstrekt zijn. Er mogen niet meer persoonsgegevens verwerkt worden dan noodzakelijk.
2. Elke betrokkene heeft recht om te weten wat er over hem is vastgelegd. Het recht op inzage (en afschrift, correctie of vernietiging) beperkt zich tot de eigen gegevens.
3. Het opvragen of verstrekken van gegevens aan derden gebeurt hetzij op basis van een wettelijke grond, hetzij op basis van bewuste toestemming van de betrokkene. Als bewuste toestemming vereist is, maar dringend noodzakelijke hulpverlening niet op gang kan komen omdat toestemming geweigerd wordt, dan biedt de wet mogelijkheden om alsnog de benodigde gegevens te verwerken.

Jeugdzorg in Eemnes

De gemeente Eemnes werkt voor jeugdzorg niet in HBEL-verband, maar binnen de regio Eemland, met de gemeente Amersfoort als centrumgemeente. Eemnes heeft een Verordening jeugdhulp vastgesteld, die samen met een set nadere regels het kader vormt voor de jeugdhulp in Eemnes. Zo hebben ook de gemeente Blaricum en de gemeente Laren elk een verordening en een set nadere regels. Blaricum en Laren hebben alle activiteiten in het sociaal domein bij Huizen belegd. Eemnes heeft voor de Wmo en de Participatiewet dezelfde samenwerking met Huizen, maar heeft voor de jeugdhulp dus een andere samenwerkingsvorm, met Amersfoort. Het frontoffice voor jeugdzorg is bij de gemeente Eemnes gebleven en wordt uitgevoerd door het Jeugd- en Gezinsteam binnen de BEL Combinatie. De backoffice, dat wil zeggen de administratie en inkoop, heeft Eemnes belegd bij de gemeente Amersfoort. Het privacyprotocol geldt niet voor de uitvoering door Amersfoort; het is niet opgenomen in de dienstverleningsovereenkomst[13] met Amersfoort en is ook niet op een andere wijze vastgelegd. De dienstverleningsovereenkomst beschrijft dat Amersfoort de taken voor Eemnes uitvoert volgens de Amersfoortse protocollen, kwaliteitsstandaarden en procedures. Uit gesprekken met betrokkenen blijkt dat de BEL Combinatie ervan uitgaat dat in Amersfoort ongeveer dezelfde regels worden gehanteerd als in Huizen, waar de overige uitvoering voor de BEL-gemeenten plaatsvindt. Dit is in het kader van dit rekenkameronderzoek niet gecontroleerd. Specifiek voor Eemnes zijn er afspraken gemaakt binnen het Jeugd- en Gezinsteam over de omgang met privacy. Deze afspraken zijn niet vastgesteld door het college van Eemnes, maar bestaan uit vastgelegde interne afspraken van het Jeugd- en Gezinsteam[14], gemaakt naar aanleiding van een training over privacy en op basis van de Handreiking Privacy Sociale (wijk)teams Eemland.[15]

Normen	Score
De BEL-gemeenten hebben de uitgangspunten voor het privacybeleid beschreven en vastgesteld	De gemeenten voldoen
De BEL-gemeenten (dan wel de uitvoerende gemeente[16]) hebben de risico's voor het beheer, gebruik en de uitwisseling van persoonsgegevens (voor de drie decentralisaties) onderzocht.	De gemeenten voldoen niet

[13] Gemeente Amersfoort, Dienstverleningsovereenkomst Sociaal Domein 2015 en 2016, gemeente Amersfoort en gemeente Eemnes, 7 maart 2016, artikel 9, lid 2.
[14] Gemeente Amersfoiort, Privacy afspraken Jeugd- en Gezinsteam n.a.v. Privacy Training (april 2015), 23 april 2015
[15] Regio Eemland, Lydia Janssen, Handreiking Privacy Sociale (wijk)teams Eemland, voorjaar 2015.
[16] De uitvoerende gemeente is de gemeente die de betreffende (deel)taak in het sociaal domein uitvoert in opdracht van de gemeente Blaricum, Eemnes en/of Laren. Het kan gaan om Huizen (als centrumgemeente in HBEL-verband), om Amersfoort of om Eemnes (jeugdzorg voor Eemnes).

Normen	Score
De BEL-gemeenten (dan wel de uitvoerende gemeente) hebben normen voor het beheer, het gebruik en de uitwisseling van persoonsgegevens door medewerkers van de gemeente en andere betrokken partijen.	De gemeenten voldoen deels

2.2 De Wet bescherming persoonsgegevens

Deze paragraaf gaat in op de volgende onderzoeksvraag:
Voldoen deze richtlijnen en beleidsregels aan de bepalingen uit de Wet bescherming persoonsgegevens?

Het privacyprotocol

Het privacyprotocol en de gehanteerde richtlijnen binnen BEL richten zich op de praktische invulling van het werkproces binnen het sociaal domein. De belangrijkste punten van het privacyprotocol zijn een vertaling van twee van de belangrijkste punten van de Wbp volgens de Autoriteit Persoonsgegevens.

> privacyprotocol: *de verwerking van persoonsgegevens moet passen binnen het doel waarvoor deze verstrekt zijn. Er mogen niet méér persoonsgegevens verwerkt worden dan noodzakelijk;*
>
> Autoriteit Persoonsgegevens (subnorm b): *Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn.*
>
> privacyprotocol: *elke betrokkene heeft recht om te weten wat er over hem is vastgelegd. Het recht op inzage (en afschrift, correctie of vernietiging) beperkt zich tot de eigen gegevens;*
>
> Autoriteit Persoonsgegevens (subnorm c): *Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking.*

Overige beleidsstukken en richtlijnen

De zorgvuldige manier van verwerken van persoonsgegevens blijkt uit de inrichting van de werkprocessen. Uit alle beleidsstukken en richtlijnen valt te destilleren dat deze zijn opgesteld vanuit de bestaande wetgeving. Het Handboek Informatiebeveiliging kent een hoofdstuk ‘Beheer van bedrijfsmiddelen’ waarin de procedures voor toegang en autorisatie voor systemen beschreven zijn. Ook de uitgebreide specifieke protocollen rondom Basisregistratie Personen zijn van toepassing op het sociaal domein. Het Handboek Informatiebeveiliging richt zich op de inrichting van verscheidene werkprocessen, zoals de autorisatieprotocollen voor verschillende

systemen binnen de BEL combinatie, maar dit Handboek is alleen van toepassing op de BEL Combinatie. De uitvoering van de taken van het sociaal domein vindt voornamelijk plaats bij de gemeenten Amersfoort en Huizen. In de dienstverleningsovereenkomst tussen Eemnes en Amersfoort voor de jeugdzorg ligt expliciet vast dat Amersfoort zich dient te houden aan de Wet bescherming persoonsgegevens.[17] Voor de andere afspraken tussen de uitvoerende gemeenten en de BEL-gemeenten en de regels en richtlijnen van de uitvoerende gemeenten, zie de volgende paragraaf.

Normen	Score
De richtlijnen en beleidsregels voldoen aan de belangrijkste bepalingen uit de Wet bescherming persoonsgegevens:[18] a) Persoonsgegevens mogen alleen in overeenstemming met de wet en op een behoorlijke en zorgvuldige manier worden verwerkt. b) Persoonsgegevens mogen alleen voor welbepaalde, vooraf uitdrukkelijk omschreven en gerechtvaardigde doeleinden worden verzameld. En vervolgens alleen verder worden verwerkt voor doeleinden die daarmee verenigbaar zijn. c) Degene van wie persoonsgegevens worden verwerkt (de betrokkene genoemd), moet ten minste op de hoogte zijn van de identiteit van de organisatie of persoon die deze persoonsgegevens verwerkt (de zogeheten verantwoordelijke) en van het doel van de gegevensverwerking. d) De gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.	De gemeenten voldoen

2.3 Toezicht op privacyborging

Deze paragraaf gaat in op de volgende onderzoeksvraag:
Hoe zien de BEL-gemeenten erop toe dat de juridische borging van de privacy van een voldoende niveau is en blijft?

Drie gemeenten betrokken bij de uitvoering

De verwerking van persoonsgegevens voor het sociaal domein vindt plaats in Huizen, Amersfoort en het Jeugd- en Gezinsteam in Eemnes. De samenwerking met Huizen vindt plaats binnen een gemeenschappelijke regeling: SoZa HBEL.

[17] Gemeente Amersfoort, Dienstverleningsovereenkomst Sociaal Domein 2015 en 2016, gemeente Amersfoort en gemeente Eemnes, 7 maart 2016, artikel 9, lid 1c.
[18] De gemeenten dienen te voldoen aan alle bepalingen in de Wbp. Voor dit korte onderzoek operationaliseren we dit in de vier belangrijkste bepalingen zoals de Autoriteit Persoonsgegevens die zelf aanduidt.

Dienstverleningsovereenkomst Eemnes-Amersfoort

De samenwerking met Amersfoort is vastgelegd in een Dienstverleningsovereenkomst (DVO). Een belangrijke bepaling in dit kader uit de Dienstverleningsovereenkomst is artikel 9.1.b. :

> ***Artikel 9 Kwaliteit***
>
> 1. *Opdrachtnemer spant zich in om gedurende de duur van deze DVO om:*
> *b. Zich te houden aan de toepasselijke wet- en regelgeving, waaronder in ieder geval de Wet bescherming persoonsgegevens en de Wet Basisregistratie personen.*

Hiermee legt de gemeente Eemnes aan de gemeente Amersfoort op dat de gemeente Amersfoort zich moet houden aan de toepasselijke wet- en regelgeving. Daarop volgt een nadere bepaling in hetzelfde artikel:

> 2. *Opdrachtnemer spant zich in om de taken voor de opdrachtgever uit te voeren volgens de protocollen, kwaliteitsstandaarden en procedures zoals zij deze voor zichzelf hanteert, bedrijfsvoeringstaken hierbij inbegrepen.*

De gemeente Eemnes geeft hier aan Amersfoort de vrijheid om de uitvoering van desbetreffende taken uit te voeren zoals Amersfoort dat gewend is. Amersfoort hoeft expliciet niet te voldoen aan de protocollen, kwaliteitsstandaarden en procedures, zoals die in de BEL Combinatie gewoon zijn. Een dergelijk vastgelegd protocol voor het sociaal domein kent de gemeente Amersfoort niet. Dat betekent dat het privacyprotocol niet van toepassing is op de uitvoering van de taken in Amersfoort.

SoZa HBEL

De samenwerking met Huizen als centrumgemeente is vastgelegd in de gemeenschappelijke regeling Samenwerking Sociale Zaken HBEL uit 2008. De uitvoering van de Participatiewet en de Jeugdzorg zijn ook onderdeel gaan uitmaken van deze gemeenschappelijke regeling (GR). Dit volgt uit de bepaling in de GR dat dat de GR, en daarmee de gemeente Huizen, ook nieuwe wet- en regelgeving op het gebied van zorg en welzijn zal uitvoeren.[19] Middels een bijlage wordt duidelijk voor welke wetten en regelingen de GR ingericht is. Er is wel in opgenomen dat de gemeente Huizen verantwoordelijk is voor de bewaring en het beheer van de archiefbescheiden. Dit in tegenstelling tot de DVO van Eemnes en Amersfoort waarbij is opgenomen dat de gemeente Eemnes verantwoordelijk blijft voor de archivering conform de Archiefwetgeving. Fysieke dossiers blijven bij de gemeente Eemnes, de gemeente Amersfoort maakt enkel gebruik van werkdossiers.[20]

Applicaties en beveiliging

De drie gemeenten maken gebruik van afgeschermde systemen voor het totale werkproces inclusief de verwerking van persoonsgegevens. Hiervoor geldt dat de medewerkers geautoriseerd moeten zijn voor toegang en gebruik van het systeem. Ook zijn er controlemechanismen op deze

[19] Samenwerking Sociale Zaken HBEL, Artikel 2.3.
[20] Gemeente Amersfoort, Dienstverleningsovereenkomst Sociaal Domein 2015 en 2016, gemeente Amersfoort en gemeente Eemnes, 7 maart 2016, artikel 15.2

systemen, zodat inzichtelijk gemaakt kan worden, wie welke informatie geraadpleegd of gewijzigd heeft.

Naar verwachting stelt het college van Huizen binnenkort een beveiligingsplan voor data-uitwisseling binnen de gemeente vast.[21] Het uitgangspunt bij de uitvoering binnen het sociaal domein is: één gezin, één consulent en één plan. Deze werkwijze vraagt om informatie-uitwisseling en borging van een zorgvuldig gebruik van gegevens. De gemeente Huizen vertaalt deze werkwijze op dit moment naar de ICT-ondersteuning. Concreet wordt de vakapplicatie (klantinformatiesysteem) waarin consulenten hun werk doen, nu voorzien van een regie-module die overzicht biedt en informatie vastlegt.[22]

Beveiligd mailen

Voor de uitvoerende gemeenten geldt ook dat zij gebruik maken van beveiligd mailverkeer. Op die manier is de kans verkleind dat er privacygevoelige informatie via mailverkeer wordt uitgewisseld. Dit omdat mailverkeer kwetsbaar is. In Huizen en Amersfoort is het doorgevoerd vooruitlopend op landelijke voorzieningen vanuit VNG voor het beveiligd uitwisselen van gegevens met partners anders dan collega-overheden (zie verder paragraaf 2.6). In Amersfoort is het beveiligd mailen ingesteld na het datalek van januari 2016.

Functionaris voor Gegevensbescherming

Huizen, Amersfoort noch de BEL Combinatie hebben een geregistreerde functionaris voor gegevensbescherming (FG).[23] Alleen de gemeente Amersfoort is van deze drie organisaties vermeld in het register, met een vacature voor een FG. Een FG is een interne toezichthouder op de verwerking van persoonsgegevens. Hij houdt binnen de eigen organisatie toezicht op de toepassing en naleving van de Wbp. Een FG moet geregistreerd worden bij de Autoriteit Persoonsgegevens (AP) waarna de meldingsplicht voor de verwerking van persoonsgegevens bij de AP komt te vervallen, deze moeten dan voortaan bij de FG gemeld worden. Op dit moment is een FG nog niet verplicht. Voor overheidsinstanties zal een FG verplicht worden als op 28 mei 2018 de Europese verordening gegevensbescherming in werking zal treden.

CISO

De CISO van de BEL Combinatie is de functionaris die zicht zou moeten hebben op de borging van privacy. Door de constructie waarbij de uitvoering in Huizen en in Amersfoort ligt, staat hij echter op afstand. In beginsel zouden de CISO's van deze gemeenten toezicht moeten houden op de informatieveiligheid. Hierover zijn echter geen afspraken gemaakt; er is nog geen contact over geweest tussen de CISO's van de BEL Combinatie, Huizen en Amersfoort. De BEL Combinatie toetst nu dus niet of Huizen en Amersfoort zich aan de gestelde normen houden. De binnenkort door de CISO uit te voeren GAP-analyse moet nader inzicht geven in eventuele tekortkomingen.

[21] Beveiligingsplan Gebruik, koppeling en beveiliging van registratie Gegevensmakelaar, GBA-Ven vakapplicaties MZ, Gemeente Huizen, Dienst Maatschappelijke Zaken, november 2016, vastgesteld

[22] Collegevoorstel van 2 december 2016, voorgesteld besluit: 1. Toestemming geven voor het gebruik van persoonsgegevens uit de gemeentelijke Gegevensmakelaar en de GBA-V door medewerkers van de dienst Maatschappelijke Zaken; 2. Vaststellen van het beveiligingsplan.

[23] https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/functionaris-voor-de-gegevensbescherming Register geraadpleegd op 30-11-2016 om 13:43 uur.

Normen	Score
De BEL-gemeenten en de uitvoerende gemeente hebben afspraken gemaakt over de bescherming van gegevens, bijvoorbeeld over werkvoorschriften, procedures en protocollen voor het gebruiken, uitwisselen en bewaren van persoonsgegevens.	De gemeenten voldoen deels
De BEL-gemeenten houden toezicht op de juridische borging van privacy.	De gemeenten voldoen niet

2.4 Communicatie met inwoners

Deze paragraaf gaat in op de volgende onderzoeksvraag:
Hoe communiceren de BEL-gemeenten naar burgers over de wijze waarop zij omgaan met persoonsgegevens?

Informatie op de website
De vier gemeenten in HBEL-verband hebben elk het Privacyprotocol Sociaal Domein HBEL (privacyprotocol) vastgesteld. Dit document is ook terug te vinden op de website van Maatschappelijke Zaken HBEL, de uitvoeringsorganisatie in Huizen. Onder 'Over deze website' wordt het vraagstuk privacy besproken. Hier is te vinden waarom de gemeenten gegevens verzamelen, om welke gegevens het gaat, wat er met die gegevens gebeurt en hoe een inwoner een klacht hierover kan indienen bij de gemeente Huizen. Hier bevindt zich ook de link naar het privacyprotocol. Ook het Jeugd- en Gezinsteam van Eemnes heeft deze informatie op haar website staan evenals een link naar het privacyprotocol.

Toestemmingsverklaring
Zowel in Huizen als bij het Jeugd- en Gezinsteam in Eemnes, moeten inwoners een toestemmingsverklaring indienen als zij gebruik (willen) maken van de diensten binnen het sociaal domein. In het geval van Huizen heeft het formulier een bijlage waarin beschreven wordt waarom de gemeente persoonsgegevens verwerkt; welke kaders de wet daarvoor meegeeft; wat de uitgangspunten van de gemeente hieromtrent zijn en wat de gemeente en de inwoner van elkaar mogen verwachten. Daarnaast geeft de bijlage een opsomming van de rechten van de inwoner met betrekking tot zijn/haar gegevens. Tot slot een verwijzing naar de mogelijkheid tot het indienen van een klacht bij de gemeente Huizen.

Cliëntenraad
Naast bovenstaande algemene manieren om inwoners te wijzen op het privacyprotocol heeft de gemeente Huizen ook met diverse cliëntenraden gesproken over privacy. Bijvoorbeeld met de Cliëntenraad Participatiewet HBEL, de Wmo-raad Huizen en SamenKracht, een cliëntenraad op regionaal niveau.

Calamiteitenprotocol
De calamiteitenprotocollen jeugd van zowel Eemnes als de Regio Gooi & Vecht zijn mede gericht op communicatie in het geval van een calamiteit of incident. Hierbij wordt ook rekening gehouden met privacy: het gaat om communicatie naar buiten, naar derden en dat geeft beperkingen in de soort informatie die gedeeld mag en kan worden. Maar ook binnen het calamiteitenoverleg mag enkel de benodigde informatie gedeeld worden, wat veelal procedurele informatie is.

Uitvoering
Er zijn in Huizen zes kwaliteitsmedewerkers die op basis van het kwaliteitsplan consulenten voor het sociaal domein begeleiden en controleren. Uit gesprekken blijkt dat de gemeente Huizen geen managementinformatie verzamelt over privacy-issues die zich voordoen in de uitvoering voor Huizen of de BEL-gemeenten. Het is daarom niet inzichtelijk in hoeverre de gemeente zich houdt aan het privacyprotocol. Daarmee is overigens niet gezegd dat de gemeente zich niet houdt aan het protocol, of geen oog heeft voor privacy-issues. Hetzelfde geldt voor de gemeente Amersfoort.

Normen	Score
De BEL-gemeenten hebben een passend protocol voor het communiceren over de omgang met persoonsgegevens.	De gemeenten voldoen

2.5 Informatie-uitwisseling met ketenpartners

Deze paragraaf gaat in op de volgende onderzoeksvraag:
Hoe gaan de BEL-gemeenten om met privacygevoelige gegevens in het sociaal domein, mede gelet op de informatie-uitwisseling met ketenpartners?

Gevolgen van de decentralisaties
Betrokkenen geven aan dat de situatie door de decentralisaties veranderd is. De gemeente werkt met meer organisaties samen. Vroeger werd veel met subsidies werd geregeld en had de gemeente geen zicht op cliëntgegevens. Nu is vaker sprake van een opdrachtgever-opdrachtnemer relatie, waarbij de gemeente vanwege de facturering of verantwoordingsrapportages ook zicht zou kunnen krijgen op privacygevoelige gegevens. Dit wordt zoveel mogelijk tegengegaan door het hanteren van codes en het vermijden van het gebruik van persoonsnamen. Maar in de praktijk ligt hier een risico. Ook het beginsel van ‘één gezin – één plan’ zorgt ervoor dat meer dan voorheen persoonsgegevens van cliënten onderling worden gedeeld en besproken binnen de gemeente. De administratie en uitvoering door de gemeenten zijn inmiddels volgens de landelijke richtlijnen[24] ingericht, waardoor de privacyrisico’s daar geminimaliseerd zijn.

Afspraken met ketenpartners
Betrokkenen geven aan dat in de afspraken met ketenpartners zaken nog steviger ingericht kunnen worden. Het privacyprotocol geldt alleen voor de gemeenten, niet voor ketenpartners. Het is dus niet van toepassing op de verstrekking van gegevens aan de gemeente door andere partijen (bijvoorbeeld zorgaanbieders, scholen of ‘Veilig Thuis’). Welke informatie zij mogen verstrekken wordt bepaald door de privacywetgeving waaronder de betreffende partij valt, en hun eigen privacyregelingen.[25]

In de praktijk blijkt dat ketenpartners soms makkelijker dan de gemeente zijn in het delen van informatie. Het is voor velen nog wennen om om te gaan met de nieuwe werkwijzes en richtlijnen. Zo zijn er bijvoorbeeld leraren die zich zorgen maken over een kind en dan met vermelding van een persoonsnaam vragen of dat kind bekend is bij het Jeugd- en Gezinsteam. Dat is echter informatie die de gemeente niet mag verstrekken. Zowel in Huizen als in Eemnes/Amersfoort wordt aangestipt dat de kennis van privacywetgeving bij ketenpartners soms te kort schiet. Betrokkenen

[24] Onder meer Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG), de Wet bescherming persoonsgegevens en daarmee samenhangende regelgeving.
[25] Zie ook het Privacy Protocol Sociaal Domein HBEL.

in zowel Huizen als in Eemnes/Amersfoort stellen dat gemeente daar aandacht aan moet schenken.[26]

Normen	Score
De afspraken rond informatie-uitwisseling met ketenpartners zijn duidelijk en passend.	De gemeenten voldoen deels
BEL-gemeente, uitvoerende gemeente en ketenpartners zijn op de hoogte van de afspraken en handelen ernaar.	De gemeenten en ketenpartners voldoen deels

2.6 Risico's

Deze paragraaf gaat in op de volgende onderzoeksvraag:
Welke risico's zijn te onderkennen in de huidige wijze waarop de privacy van burgers juridisch geborgd is binnen de BEL-gemeenten?

Managementinformatie over risico's en incidenten
Zoals in paragraaf 2.4 is beschreven verzamelt Huizen geen managementinformatie over privacygerelateerde issues. Dat maakt dat Huizen hierover niet rapporteert aan de BEL-gemeenten. Zowel Huizen als de BEL Combinatie geven aan dat er nog geen privacy-issues zijn geweest. In Eemnes is in het verleden een voorval geweest waarbij een beschikking is gestuurd naar het mailadres van een ouder van een ander kind dan bedoeld.[27]

Risico's en risicobewustzijn
De gesprekken bevestigen dat de BEL Combinatie als opdrachtgevende organisatie op afstand staat van de uitvoering. Dat is ook zichtbaar in het bewustzijn van en de omgang met risico's. De BEL Combinatie heeft geen afspraken met Huizen en Amersfoort over in welke gevallen de BEL-gemeenten informatie ontvangen over privacygerelateerde incidenten[28].

Uit de gesprekken met Huizen en Eemnes/Amersfoort blijkt dat er zowel op managementniveau als ook in de uitvoering bewustzijn is van de risico's. Dit zijn overigens voor een belangrijk deel geen nieuwe risico's voor de uitvoerende organisaties. Men heeft al vele jaren ervaring in de omgang met vertrouwelijke persoonsgegevens; het is als het ware een kernactiviteit van de uitvoeringsorganisaties in het sociaal domein. Wel is het zo dat het belang van een goede privacyborging steeds groter geacht wordt. Dit onder meer omdat identiteitsfraude en andere vormen van fraude met persoonsgegevens grotere vormen kunnen aannemen. Voor de uitvoeringsorganisaties van de BEL-gemeenten in Huizen en Eemnes/Amersfoort is dit een reden om scherp te zijn op mogelijke privacy-issues. Beide uitvoeringsorganisaties geven fictieve en niet-fictieve voorbeelden van voorvallen. Het gaat niet om daadwerkelijke incidenten, maar om voorvallen waarbij betrokkenen bij de uitvoering informatie dreigen te delen die ze niet mogen delen. De neiging om informatie te delen komt vrijwel altijd voort uit de wens om het eigen werk zo goed mogelijk te doen. Om iemand met een hulpvraag zo goed mogelijk te helpen of om een evident fraudegeval aan het licht te brengen. De voorvallen tonen de complexiteit van het werken met privacygevoelige informatie in het sociaal domein aan en daarmee het risico dat het een keer fout gaat.

[26] In meerdere interviews komt dit punt terug.
[27] Dit specifieke voorval is niet recent en is in het kader van dit rekenkameronderzoek niet nader onderzocht.
[28] Privacygerelateerde incidenten: voorvallen waarbij sprake is van een inbreuk op de privacy.

Meerdere betrokkenen noemen de volgende interne aandachtspunten voor privacy:

- beveiligd mailen;
- postproces.

Het beveiligen van het mailverkeer is een aspect dat in 2016 aandacht heeft gekregen, zowel in Huizen als in Eemnes/Amersfoort. Het is echter nog in ontwikkeling. Zo loopt bijvoorbeeld het contact met huisarts en zorgarts via een beveiligde mailapplicatie, maar met sommige andere instanties, zorgaanbieders en andere ketenpartners is dat niet het geval (zie ook paragraaf 2.3).

Een ander aandachtspunt is de afhandeling van de post door de postkamer. In Huizen is er voor gekozen dat twee medewerkers van de postkamer zich bezig houden met de poststukken voor jeugdzorg.

Meldplicht datalekken en het datalek in Amersfoort

Voor gemeenten geldt dat er sinds 1 januari 2016 een wettelijke plicht is om ernstige datalekken te melden. Dat wil zeggen dat de gemeente een inbreuk alleen hoeft te melden als deze leidt tot een aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.[29] Het is aan de gemeente om te bepalen of een binnen de organisatie ontdekt datalek binnen de reikwijdte valt van de meldplicht datalekken aan de Autoriteit Persoonsgegevens.

In Amersfoort vond op 28 januari 2016 een datalek in het sociaal domein plaats door het verzenden van een fout geadresseerde mail.[30] Amersfoort meldde dit pas op 7 april 2016 aan de Autoriteit Persoonsgegevens (AP), nadat de AP hierover – ingeseind door de onterechte ontvanger - zelf contact opnam met de gemeente. Hoewel dit voorval geen betrekking heeft op het sociaal domein in de BEL-gemeenten, maakt het duidelijk waar in Amersfoort de kwetsbaarheden lagen. Dezelfde kwetsbaarheden gelden – in ieder geval deels – ook voor de BEL-gemeenten. Het in Huizen ingestelde beveiligd mailen en de instructies daarover vormen een borging tegen datalekken. Het is echter de vraag of de gemeente daarmee het per ongeluk verzenden van een mail aan de verkeerde ontvanger kan voorkomen. In Amersfoort ontbrak een afwegingskader en een protocol voor het melden van datalekken. Daardoor zijn onjuiste aannames gedaan, diverse fouten gemaakt en is het datalek laat gemeld. De BEL Combinatie geeft aan dat binnen de eigen organisatie bekend is hoe en bij wie informatiebeveiligingsincidenten moeten worden gemeld en hoe ze worden geregistreerd. Verder is er een procedure voor de afhandeling van de gemelde incidenten. Het betreft een recent door de regio vastgestelde procedure en het is niet duidelijk in hoeverre deze procedure ook in Huizen is geïmplementeerd.[31] Vanaf mei 2018 moeten gemeenten een gemeentebrede functionaris informatiebeveiliging hebben. Zoals in paragraaf 2.3 aangeduid, zijn er, net als in Amersfoort, in de BEL Combinatie en in Huizen nog geen gemeentebrede functionarissen gegevensbescherming benoemd. Voor de BEL Combinatie neemt de CISO deze taken voor zijn rekening, maar dit betreft niet de informatiebeveiliging voor het sociaal domein, aangezien de verantwoordelijkheid daarvoor bij Huizen en Amersfoort ligt.

Meldcultuur en meldingsbereidheid

Er zijn in de BEL-gemeenten geen incidenten bekend. Mede naar aanleiding van het datalek in Amersfoort zijn protocollen en procedures opgesteld om privacy-issues te voorkomen. Het

[29] Wet bescherming persoonsgegevens, artikel 34a, eerste lid.
[30] Verdonck, Klooster & Associates, Frank van Vonderen, Extern onderzoek datalek, gemeente Amersfoort, 13 juni 2016.
[31] Regio Gooi en Vechtstreek, Interne procedure afhandeling meldingen datalekken, 5 juli 2016 (datum vaststelling onbekend).

management geeft aan dat het voor medewerkers veilig is om voorvallen te melden. Het is echter niet duidelijk in hoeverre er op dit moment sprake is van een open meldcultuur. De aandacht ligt vooral bij het voorkomen van voorvallen en bij het actie ondernemen bij een voorval. Dit onderzoek geeft geen inzicht in hoeverre een medewerker van een uitvoeringsorganisatie gestimuleerd wordt om melding te doen van een door hem of haar gemaakte fout, in hoeverre de medewerkers daadwerkelijk beschermd worden en hoe de perceptie van medewerkers hierover is. Het creëren van een meldcultuur heeft de aandacht, zo blijkt uit meerdere gesprekken, maar het is nog in ontwikkeling.

Bestuurlijke risico's

In het Calamiteitenprotocol Jeugd is opgenomen dat bestuurders in verband met de bestuurlijke verantwoordelijkheid informatie mogen ontvangen over hoe het systeem heeft gewerkt en welke partijen een aandeel hebben gehad in de zorg. De recent vastgestelde interne meldprocedure geeft ook aan op welke wijze de verantwoordelijke bestuurders betrokken worden.[32] Bestuurders mogen overigens daarbij geen privacygevoelige informatie inzien. Omdat er in de BEL-gemeenten vooralsnog geen zwaarwegend voorval is geweest, is er nog geen ervaring met het betrekken en informeren van bestuurders hierover. Het voorval in Amersfoort leert dat het inschatten van politiek-bestuurlijke implicaties lastig is.

Normen	Score
De uitvoerende gemeente rapporteert aan de BEL-gemeenten over de diverse typen risico's rond informatiebeveiliging en privacy.[33]	De gemeenten voldoen niet
De BEL-gemeente is zich bewust van de risico's; dit is te zien in beheersmaatregelen.	De gemeenten voldoen deels

[32] Regio Gooi en Vechtstreek, Interne procedure afhandeling meldingen datalekken, 5 juli 2016 (datum vaststelling onbekend).
[33] Zie paragraaf 1.2, vraag 6 voor een opsomming van de risico's.

3. Conclusies en aanbevelingen

3.1 Conclusies

De Rekenkamer BEL heeft de volgende hoofdvraag geformuleerd:
Hoe is in het licht van de toegenomen decentralisatie en verdergaande digitalisering de privacy van burgers juridisch geborgd binnen de gemeenten Blaricum, Eemnes en Laren en op welke punten behoeft dit verbetering?

Blaricum, Eemnes en Laren hebben samen met Huizen een intergemeentelijke afdeling Maatschappelijke Zaken ingericht. De gemeente Huizen geeft invulling aan de uitvoeringsorganisatie voor het sociaal domein voor de BEL Combinatie, met uitzondering van jeugdzorg van Eemnes. De BEL-gemeenten hebben de borging van privacy daarmee op afstand gezet. Dat neemt niet weg dat de colleges van B&W van Blaricum, Eemnes en Laren zelf eindverantwoordelijk zijn voor de kwaliteit van de privacyborging voor hun inwoners.

De beleidsmatige juridische borging van de privacy van burgers is zichtbaar in het Privacyprotocol Sociaal Domein HBEL, het Handboek Informatiebeveiliging en de ambtseed. Deze voldoen aan de Wet bescherming persoonsgegevens en de Basisregistratie personen. Het privacyprotocol is online raadpleegbaar en voorziet op die manier in een passieve informatievoorziening aan inwoners. De actieve informatievoorziening vindt plaats op het moment dat inwoners gebruik gaan maken van de diensten binnen het sociaal domein. De gemeente Huizen maakt op verschillende manieren inzichtelijk waarom gegevens verwerkt worden en welke mogelijkheden inwoners daarbij hebben. Het Jeugd- en Gezinsteam Eemnes heeft dezelfde informatie en een link naar het privacyprotocol op zijn website. In geval van calamiteiten is er in Huizen en in Amersfoort oog voor privacy van de inwoners van de BEL-gemeenten.

Het Privacyprotocol Sociaal Domein, het Handboek Informatievoorziening en de ambtseed zijn gericht op de intergemeentelijke uitvoeringsorganisatie en hebben geen status voor de ketenpartners; er is geen uniform beleid ten aanzien van privacy in de gehele keten. Elke partner heeft eigen regels en richtlijnen, waarbij de gemeente soms optreedt als informeel adviseur. Het privacyprotocol is een gezamenlijk product van Huizen, Blaricum, Eemnes en Laren, maar niet van toepassing op Amersfoort. Voor Amersfoort is de bepaling opgenomen dat Amersfoort moet voldoen aan de relevante wet- en regelgeving.

Zowel Huizen als de BEL Combinatie geven aan dat er de afgelopen jaren geen privacy-issues zijn geweest. Eemnes heeft één voorval met een verkeerd geadresseerde e-mail gehad.

Er is een aantal verbeterpunten. Zo is er geen managementinformatie vanuit de uitvoerende gemeenten richting de BEL-gemeenten. De BEL Combinatie staat op afstand en heeft geen zicht op de risico's. De BEL-gemeenten zijn voor hun informatie afhankelijk van de initiatieven uit de uitvoerende organisaties. Om deze in beeld te krijgen moet de CISO een *GAP*[34]- en risicoanalyse uitvoeren, maar dit is nog niet gebeurd vanwege een capaciteitstekort.
Enkele verbeteringen zijn al zichtbaar in de BEL- (en de HBEL-) organisatie; zo wil de CISO graag samenwerken met de CISO's uit Huizen en Amersfoort. Het beveiligd mailen is in de zomer van 2016 ingevoerd, waardoor er een risico aanzienlijk is ingeperkt. Ten slotte is er op meerdere

[34] De GAP-analyse is een methode om een vergelijking te maken tussende huidige situatie en de gewenste situatie, In dit geval gaat het om een analyse over de mate waarin de gemeente de maatregelen uit de baseline Informatiebeveiliging Nederlandse Gemeenten heft ingevoerd.

niveaus binnen de uitvoeringsorganisatie oog voor het belang van het creëren van een meldcultuur. Men beseft dat dit een ingewikkeld proces is, dat niet draait om strikte procedures met verwijzingen naar sancties, maar om een procedure waarin medewerkers zich veilig voelen eventuele datalekken te melden.

3.2 Aanbevelingen

De Rekenkamer BEL komt tot de volgende aanbevelingen:

Aan de gemeenteraden:

7. De aanbeveling van de Rekenkamer BEL uit 2015 over de uitvoering van een *GAP*- en risicoanalyse met betrekking tot digitale veiligheid is nog steeds actueel. [35] Vraag het college om de CISO de *GAP*- en risicoanalyse te laten uitvoeren en laat u informeren over de uitkomst.
8. Vraag het college om managementinformatie over de risico's rond privacy en informatiebeveiliging.

Aan de colleges van B en W:

9. Stimuleer het 'veilig' melden van datalekken. Zorg voor registratie van voorvallen en bijna-voorvallen met betrekking tot privacy, met uitsluitend als doel om daarvan te leren en te verbeteren. Medewerkers moeten te allen tijde incidenten kunnen melden zonder risico op persoonlijke consequenties.
10. Breid het beveiligd mailen uit tot alle relevante ketenpartners in het sociaal domein. Evalueer de toepassing van het beveiligd mailen en betrek daarbij zowel de ervaring van de gemeenten als van de ketenpartners.
11. Onderzoek de werking en toepassing van het privacyprotocol in de praktijk. Breng in kaart waar de gemeentelijke uitvoeringsorganisatie knelpunten ervaart.
12. Onderzoek in hoeverre er verschillen zijn tussen de privacyreglementen van ketenpartners en het privacyprotocol van de BEL-gemeenten. Breng in kaart waar de ketenpartners knelpunten ervaren. Leg vast dat ook voor ketenpartners het privacyprotocol van de BEL-gemeenten als richtlijn geldt.

[35] Rekenkamer BEL, BEL op weg naar BIG, Digitale veiligheid BEL-gemeenten, Quick Scan, augustus 2015.

Bijlage 1. Geraadpleegde personen

Arieke van Andel	Senior beleidsregisseur, gemeente Amersfoort
Saskia van den Berg	Beleidsmedewerker Maatschappelijke Zaken HBEL.
Johan Cnossen	Directeur Maatschappelijke Zaken, gemeente Huizen; Uitvoerend directeur voor de gemeenschappelijke regeling HBEL; Coördinerend directeur voor de regio Gooi en Vecht.
Hans Haverkamp	Coördinator maatschappelijke ontwikkeling BEL Combinatie
Willem Kleine Deters	Juridisch beleidsmedewerker sociaal domein BEL Combinatie
Barry Oostra	Coördinator Jeugd en Gezin Eemnes
Marc Roza	Chief information security officer (ciso) BEL Combinatie; Directiesecretaris; Adviseur beleid, bestuur & kwaliteitszorg BEL Combinatie.

Bijlage 2. Geraadpleegde documenten

- BEL Combinatie, Handboek informatiebeveiliging, versie 16 september 2015
- BEL Combinatie, Jaarverslag informatiebeveiliging 2015
- Gemeente Amersfoort, Dienstverleningsovereenkomst Sociaal Domein 2015 en 2016, gemeente Amersfoort en gemeente Eemnes, 7 maart 2016
- Gemeente Amersfoort, Privacy afspraken Jeugd- en Gezinsteam n.a.v. Privacy Training (april 2015), 23 april 2015
- Gemeente Amersfoort, Rapport Verdonck, Klooster & Associates, Frank van Vonderen, Extern onderzoek datalek, gemeente Amersfoort, 13 juni 2016.
- Gemeente Eemnes, Calamiteitenprotocol instellingen zorg voor jeugd, de gemeenten in de provincie Utrecht en de gemeenten Weesp en Wijdemeren
- Gemeente Eemnes, Jeugd- en Gezinsteam Eemnes, toestemmingsformulier
- Gemeente Huizen, Beveiligingsplan Gebruik, koppeling en beveiliging van registratie Gegevensmakelaar, GBA-Ven vakapplicaties MZ, Dienst Maatschappelijke Zaken, november 2016
- Gemeente Huizen, Blaricum, Eemnes en Laren, Privacy Protocol Sociaal Domein HBEL
- Gemeente Huizen, Collegevoorstel van 2 december 2016, voorgesteld besluit:
    - 1. Toestemming geven voor het gebruik van persoonsgegevens uit de gemeentelijke Gegevensmakelaar en de GBA-V door medewerkers van de dienst Maatschappelijke Zaken;
    - 2. Vaststellen van het beveiligingsplan.
- Gemeente Huizen, Collegevoorstel van 22 april 2015 voor het college van B&W van Huizen om kennis te nemen van en in te stemmen met het Privacyprotocol Sociaal Domein HBEL
- Gemeente Huizen, diverse documenten rond beveiligd mailen, o.a. over KPN Secure Mail
- Gemeente Huizen, Do's en don'ts voor het omgaan met persoonsgegevens
- Gemeente Huizen, Handreiking communiceren met inwoners over privacy en de verwerking van persoonsgegevens in het sociaal domein
- Gemeente Huizen, Handreiking voor consulenten, behorende bij de Toestemmingsverklaring & Bijlage
- Gemeente Huizen, Handreiking Privacy voor medewerkers
- Gemeente Huizen, Intern memo aan breed managementoverleg over beveiligde e-mail, 16 februari 2016.
- Gemeente Huizen, Lijst van (gevolgde) trainingen en cursussen
- Gevolgd of nog te volgen door: Beleidsmedewerkers, juridische kwaliteitsmedewerkers en consulenten
- Gemeente Huizen, Toelichting toestemmingsverklaring gebruik persoonsgegevens
- Gemeente Huizen, Toestemmingsverklaring gebruik persoonsgegevens
- Ministerie van BZK, Handreiking Financiën en de 3 decentralisaties, 14 februari 2014
- Regio Eemland, Lydia Janssen, Handreiking Privacy Sociale (wijk)teams Eemland, voorjaar 2015.
- Regio Gooi en Vechtstreek, Calamiteitenprotocol instellingen zorg voor jeugd, de gemeenten (Bussum, Naarden, Muiden, Hilversum), Huizen, Blaricum en Laren 2015, versie 28 april 2015
- Regio Gooi en Vechtstreek, Interne procedure afhandeling meldingen datalekken, 5 juli 2016 (datum vaststelling onbekend).
- Regio Gooi en Vechtstreek, Projectplan Regie en privacy in het sociaal domein

- Regio Gooi en Vechtstreek, Samenwerkingsafspraken Jeugdzorgregio Gooi en Vechtstreek - gecertificeerde instellingen, maart 2016
- Regio Gooi en Vechtstreek, Uitvoeringsprogramma Sociaal Domein 2014
- Regio Gooi en Vechtstreek, Verslag Werkbijeenkomst Privacy, woensdag 9 december op het Regiokantoor in Bussum
- Regio Gooi en Vechtstreek, Voorstellen Regie en privacy, 9 juni 2016
- Rekenkamer BEL, BEL op weg naar BIG, Digitale veiligheid BEL-gemeenten, Quick Scan, augustus 2015
- Rekenkamer BEL, Onderzoeksprotocol van de Rekenkamer BEL
- Samenwerking Sociale Zaken HBEL
- Wet bescherming persoonsgegevens