Rekenkamer
LANSINGERLAND

Meent 94
t 010 • 267 22 42

Postbus 70012
3000 KP Rotterdam

info@rekenkamer.rotterdam.nl
www.rekenkamer.rotterdam.nl

Gemeente Lansingerland
Gemeenteraad
d.t.k.v de griffie
Postbus 1
2650 AA BERKEL EN RODENRIJS

datum
3 oktober 2016

ons kenmerk
RL/16.14/PH/ED/SE

pagina

betreft
notiebrief informatiebeveiliging

Geacht raadslid,

Rekenkamer Lansingerland heeft op 15 december 2015 aangegeven een onderzoek te starten naar de informatiebeveiliging in de gemeente Lansingerland. Aanleiding voor dit onderzoek was de uitslag van de stemkastsessie op 9 december 2015 met de gemeenteraad, waarbij het onderwerp informatiebeveiliging als zeer relevant werd benoemd. Naar later bleek is de timing van dit onderzoek naar informatiebeveiliging niet ideaal, zoals vervolgens is aangegeven in de brief van 25 mei 2016. Momenteel zijn binnen de gemeente Lansingerland veel ontwikkelingen gaande op het gebied van informatiebeveiliging.

In 2015 heeft de gemeente Lansingerland twee inventarisaties uitgevoerd die inzicht geven in de mate waarin informatiestromen veilig door de organisatie worden beheerd. Beide inventarisaties zijn uitgevoerd door een extern bureau. Eén inventarisatie is gericht geweest op het veilig en op correcte wijze gebruiken van persoonsinformatie en het borgen van de privacy.[1] De andere inventarisatie betrof een GAP-analyse ten opzichte van de Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG). Uit deze GAP-analyse blijkt in welke mate gemeente Lansingerland voldoet aan het waarborgen van een veilige informatieomgeving.[2] Uit beide inventarisaties blijkt dat de gemeente nog veel maatregelen moet invoeren om te komen tot een veilige omgeving waarin informatie wordt opgeslagen en verwerkt. De fysieke toegang tot informatie (bijvoorbeeld de toegang tot vrijstaande computers en de server en archiefruimte) is relatief beter beveiligd. Toch moeten ook hier nog maatregelen worden genomen. Uit de inventarisatie blijkt ook dat de digitale toegang tot data (al dan niet via de website of andere informatiesystemen) tekort schiet. Zo is de H-schijf een zwakke plek, is de cryptografie onvoldoende en is onduidelijk of het netwerkbeheer voldoende is.[3] Dit beeld wordt bevestigd door recent onderzoek door internet.nl[4] naar de beveiliging van gemeentelijke websites. Dit onderzoek geeft aan dat gemeente Lansingerland als één van de slechtst

[1] BMC advies, 'Persoonsinformatie en privacy. Op weg naar adequaat uitvoeringsniveau WBP door gemeente Lansingerland, 6 juni 2016.
[2] Gemeente Lansingerland, 'Informatiebeveiligingsplan', 28 november 2015.
[3] Gemeente Lansingerland, 'GAP-analyse gemeente Lansingerland op basis van de Baseline Informatiebeveiliging Nederlandse Gemeenten', 28 november 2015.
[4] https://internet.nl/site/www.lansingerland.nl/results#

scorende gemeenten geldt.[5] In de beantwoording van raadsvragen over dit internetonderzoek geeft het college aan dat de resultaten van de internettest genuanceerd moeten worden. De slechte resultaten hebben betrekking op de domeinnaam om informatie voor burgers te publiceren. De score voor het gebruik van digitale formulieren ligt volgens het college hoger. Daarnaast geeft het college aan dat er andere testen zijn uitgevoerd waaruit blijkt dat Lansingerland positief scoort. Ook vermeldt het college dat zij de komende tijd maatregelen nemen om de informatieveiligheid zo goed mogelijk te regelen.[6]
Op basis van de inventarisaties heeft het college in november 2015 al een plan van aanpak ontwikkeld om te komen tot een verbetering van de informatiebeveiliging. De inzet van de gemeente op het onderwerp is groot. Ook het vervolgtraject is beschreven in een apart plan van aanpak. De verbeterpunten zullen worden vormgegeven in verschillende werkgroepen. Om dit verbeterproces te leiden is er een zzp'er ingehuurd. Met betrekking tot de Wet Bescherming Persoonsgegevens (WBP) zijn eveneens de hiaten in kaart gebracht door een extern bureau. Vervolgens heeft de gemeente een plan van aanpak opgesteld om op termijn volledig aan de Baseline en de wetgeving te kunnen voldoen. Als aan de Baseline wordt voldaan, is de informatiebeveiliging in opzet toereikend.
Gezien de vele verbeteractiviteiten die op het punt staan gestart te worden, kan later in het jaar meer duiding gegeven worden aan de voortgang van dit traject. De Rekenkamer Lansingerland heeft derhalve besloten om het onderzoek naar informatiebeveiliging op een later moment voort te zetten. Wel kunnen de eerste bevindingen een positieve bijdrage leveren aan het verbetertraject, waardoor de rekenkamer heeft besloten een tussentijdse rapportage op te stellen. In deze brief (de tussentijdse rapportage) wil de rekenkamer graag enkele noties over het verbeterproject meegeven. Daartoe wordt ingegaan op het beleid en het beveiligingsplan, de plannen van aanpak, de planning en het verzamelen en gebruik van persoonsgegevens.

De noties van de rekenkamer zijn gebaseerd op de relevante documenten (waarbij de rekenkamer heeft gewacht tot de definitieve versies beschikbaar waren). Deze brief is voor wederhoor aangeboden.

beleid en beveiligingsplan

informatiebeveiligingsbeleid

De gemeente Lansingerland beschikt over een informatiebeveiligingsbeleid.[7] In het gemeente breed informatiebeveiligingsbeleid van de gemeente Lansingerland wordt uiteengezet welk informatiebeveiligingsniveau op dat moment in de gemeente aanwezig is en wat wordt nagestreefd. Daartoe is vastgelegd dat het doel van informatiebeveiliging is dat de beschikbaarheid en continuïteit van systemen is geborgd, evenals de integriteit en de betrouwbaarheid van de informatie. Tevens moet de vertrouwelijkheid en controleerbaarheid van informatie door informatiebeveiliging worden geborgd. Ook is in het beleidsplan aangegeven wie waarvoor verantwoordelijk is en hoe de organisatie van de informatiebeveiligingsfunctie is ingericht. De indeling van het beleidsplan is gebaseerd op de BIG. Al de aspecten uit de BIG komen aan de orde, waarbij per aspect een algemene doelstelling, het beoogde resultaat en de basisnormen worden beschreven. Het betreft een duidelijke en inzichtelijke uitwerking. Mede doordat het beleidskader is ingedeeld naar doelstellingen per hoofdstuk uit de BIG, lijkt de

[5] http://www.ad.nl/rotterdam/websites-gemeenten-zijn-eenvoudig-te-hacken~aabec89c/
[6] Gemeente Lansingerland, beantwoording raadsvragen dhr. Bovens, 18 juli 2016
[7] Gemeente Lansingerland, 'Gemeente breed informatiebeveiligingsbeleid', 3 juli 2015.

gemeente het voldoen van de BIG als een visie te presenteren. De rekenkamer ziet de BIG echter meer als een middel om tot betere informatiebeveiliging te komen. Zij mist de visie van de gemeente waaruit blijkt welke concrete ambities de gemeente heeft voor het waarborgen van een veilige informatievoorziening en de wijze waarop informatiebeveiliging daaraan moet bijdragen. Evenmin is ingegaan op de beschikbare middelen om de doelstellingen te kunnen realiseren.

informatiebeveiligingsplan
Een nadere uitwerking van het informatiebeveiligingsbeleid is vastgelegd in het informatiebeveiligingsplan.[8] Dit plan is gebaseerd op een risicoanalyse van de bedrijfsprocessen ten opzichte van de ICT-omgeving. Het bevat aandachtspunten die moeten worden verbeterd om aan de doelstellingen van het beveiligingsbeleid, in casus de BIG, te kunnen voldoen. Daarbij vindt ook prioritering van de te nemen verbetermaatregelen plaats.

Over de uitgevoerde risicoanalyse wil de rekenkamer twee punten opmerken:

1. De gemeente stelt dat de Baseline informatiebeveiliging bestaat uit ruim 300 maatregelen, waarvan ongeveer 50% is geïmplementeerd door de gemeente. Volgens de gemeente is dit landelijk gezien een gemiddelde score. De rekenkamer heeft dit niet geverifieerd. Wel is de rekenkamer nagegaan op welke aspecten de gemeente nog niet voldoet. Wat opvalt, is dat gemeente Lansingerland vooral slecht scoort op het gebied van verwerving, ontwikkeling en onderhoud van informatiesystemen (38%), op beheer van incidenten (10%), bedrijfscontinuïtsbeheer (30%), naleving (23%) en ISMS (0%). Uit de door de gemeente uitgevoerde risicoanalyse blijkt meer gedetailleerd dat tenminste de volgende onderdelen nog moeten worden gerealiseerd:
   - Verwerving, ontwikkeling en onderhoud: bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.
   - Beheer incidenten: bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.
   - Bedrijfscontinuïteitsbeheer: tegengaan van onderbreking van bedrijfsactiviteiten en bescherming van kritische bedrijfsprocessen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.
   - Naleving: voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.
   - ISMS: Information Security Management System. De VNG heeft als product bij de BIG een praktische handleiding geleverd die beschrijft wat er nodig is om een ISMS te implementeren en te beheersen op basis van de BIG. Op deze manier kan informatieveiligheid over een langere periode op een steeds hoger niveau uitgevoerd worden. Gemeente Lansingerland heeft nog geen gedocumenteerd ISMS.

   "Daarnaast blijkt dat in de categorieën die niet tot de Baseline Informatiebeveiliging behoren (de categorieën 'mensen' en 'DIV') ook nog ontwikkelpunten zijn geconstateerd." Een voorbeeld hiervan is meer kennis en bewustzijn over informatiebeveiliging en informatieveiligheid onder medewerkers.[9]

[8] Gemeente Lansingerland, 'Informatiebeveiligingsplan', 28 november 2015.
[9] Gemeente Lansingerland, 'Informatiebeveiligingsplan', 28 november 2015.

De ontwikkelpunten zijn niet zozeer de makkelijk realiseerbare onderdelen, zoals het schrijven van een protocol, maar juist grotendeels aspecten die relatief veel tijd en aandacht vergen om te verbeteren. Naar de mening van de rekenkamer laat de risico-inventarisatie zien dat nog relatief grote inspanningen moeten worden verricht om te komen tot de beoogde resultaten. Dit lijkt het college soms te onderschatten. In het beveiligingsplan wordt bijvoorbeeld aangegeven dat de categorie mensen (in relatie tot onder meer naleving) aandacht verdient, omdat met relatief weinig inspanning een groot effect kan worden behaald. De rekenkamer is op basis van dit soort opmerkingen van mening dat de gemeente de benodigde inspanningen voor een cultuur en gedragsverandering onderschat. Juist veranderingen in houding, gedrag en cultuur vergen langdurig een grote, actieve inzet vanuit het management.[10]

2. Om te komen tot de risico-inventarisatie is gebruik gemaakt van een Risico Inventarisatie en Evaluatie. Zoals uitgelegd op blz. 6 van het informatiebeveiligingsplan van de gemeente Lansingerland, betekent dit dat het opvragen van bewijzen of toetsing in de praktijk niet plaatsvindt. Bij deze werkwijze is daarom een risico aanwezig dat het uitgangspunt voor de verbeteringen niet klopt. In het plan van aanpak zitten echter geen vangnetten of maatregelen verwerkt om mogelijk fouten in deze inventarisatie op te vangen. De rekenkamer raadt aan hier nog een kritisch naar te kijken en in het bijzonder de maatregelen waar de gemeente aangeeft reeds aan te voldoen nog eens te toetsen.[11]

plan van aanpak en verbeterplannen

Op basis van de risicoanalyse is vastgesteld welke verbetermaatregelen nog moeten worden genomen. Deze zijn al vastgelegd in het informatiebeveiligingsplan en ook in een separaat plan van aanpak[12]. Uit het plan van aanpak blijkt dat op het peilmoment augustus 2015 ten aanzien van de verschillende onderdelen van de baseline in totaal 204 verbeteracties (van de ruim 300 maatregelen) nog geheel of gedeeltelijk moeten worden uitgevoerd om aan alle normen van de baseline voor informatiebeveiliging Nederlandse gemeenten te voldoen. Het plan van aanpak vermeldt alleen de verbeteracties waaraan de gemeente in de periode 2015-2016 prioriteit gaat geven en waarvan de gemeente aangeeft deze belangrijk te vinden, aan te kunnen én waar te kunnen maken. De gemeente heeft op basis van vier criteria de belangrijkste verbeteracties geselecteerd. Hoe de gemeente tot de

[10] In ambtelijk wederhoor geeft de gemeente aan dat ambtelijk en op collegeniveau de inspanningen niet worden onderschat. Zo heef de gemeente een projectleider aangetrokken voor de implementatie van de BIG, zijn middelen vrijgemaakt en is er een specifieke portefeuillehouder benoemd. Ook is er een informatiebeveiligingscommissie die vier keer per jaar bijeen komt en heeft de gemeente zich aangesloten bij de informatiebeveiligingsdienst en wordt in het najaar een bewustwordingscampagne gestart, zo blijkt uit ambtelijk wederhoor. De rekenkamer merkt hierover op dat de gemeente zeker veel inspanningen verricht om de informatiebeveiliging te optimaliseren. Echter, een groot aantal van de geconstateerde risico's vergt inspanningen die veel inzet en een grote doorlooptijd vereisen, waardoor de beoogde afronding in 2017 niet realistisch lijkt.

[11] In ambtelijk wederhoor is door de gemeente aangegeven dat de kans op fouten in de inventarisatie klein wordt geacht. Voor de inventarisatie zijn verantwoordelijk medewerkers bevraagd. Daarna is de gehele inventarisatie door de informatiebeveiligingscommissie in gezamenlijkheid besproken.

[12] Gemeente Lansingerland, Plan van aanpak Informatiebeveiliging, Overzicht van de verbeteracties 2015/2016, 28 november 2015.

prioriteitstelling van deze criteria is gekomen is niet duidelijk. Evenmin is duidelijk in hoeverre de ontwikkelpunten zonder verbeteractie in de toekomst nog worden opgepakt. Zo wordt door het college in het plan van aanpak aangegeven dat verbeteracties die de komende periode niet worden uitgevoerd, volgend jaar (als weer een nieuwe risico inventarisatie wordt gehouden) opnieuw worden gewogen op urgentie. Deze maatregelen kunnen dan eventueel worden opgenomen in het plan van aanpak 2017.[13] Hieruit blijkt dat niet zeker is of in 2017 wel alle resterende ontwikkelpunten zullen worden opgepakt, dan wel dat ontwikkelpunten ook in 2017 niet worden verbeterd. De rekenkamer merkt hierover op dat het jaarlijks inventariseren van bestaande en nieuwe risico's ertoe kan leiden dat eerder geconstateerde ontwikkelpunten kunnen worden vergeten.
Uit het plan van aanpak en een interne presentatie over het plan van aanpak blijkt wel dat er 42 maatregelen direct geïmplementeerd zullen worden en 157 maatregelen later. Echter, voor de maatregelen die worden uitgevoerd ontbreekt een exacte planning voorzien van opleverdatum en tussentijdse mijlpalen. Met betrekking tot de aspecten van de BIG waarop gemeente Lansingerland slecht scoorde, is de gemeente van plan het volgende te ondernemen[14]:

- ISMS: wordt direct geïmplementeerd.
- Maatregelen op het gebied van beheer van incidenten worden bijna allemaal meteen geïmplementeerd.
- Verwerving, ontwikkeling en onderhoud: veelal later implementeren, op twee maatregelen na.
- Naleving: alle maatregelen later implementeren, behalve in de P&C cyclus rapporteren over informatiebeveiliging.
- Bedrijfscontinuïteitsbeheer: alles later implementeren.

Uit een impactanalyse door de gemeente blijkt dat als de geprioriteerde verbeteracties zijn genomen, er nog steeds enkele onderdelen van de BIG zijn waar de gemeente Lansingerland laag op scoort, te weten: verwerving, ontwikkeling en onderhoud (42%), bedrijfscontinuïteitsbeheer (30%) en naleving (32%).[15] Wat de betekenis hiervan is voor de informatiebeveiliging en welke risico's de gemeente hierdoor loopt, is niet inzichtelijk gemaakt. Evenmin wordt inzichtelijk op welke termijn deze tekortkomingen zullen worden opgeheven.
Om de verbeteracties te realiseren heeft gemeente Lansingerland externe deskundigheid ingehuurd. Deze deskundige heeft een eigen plan van aanpak geschreven. Volgens deze aanpak worden de maatregelen om de risico's af te dekken per hoofdstuk van de BIG uitgevoerd. De hoofdstukken en paragrafen van de BIG worden achtereenvolgens opgepakt. De eerdergenoemde verdeling, risico inschatting en geprioriteerde maatregelen zijn daarmee losgelaten. Waarom het eerdere plan van aanpak, met bijbehorende risico inschatting en prioritering van maatregelen is losgelaten, heeft gemeente Lansingerland niet in enig plan aangegeven.[16]

---

[13] Gemeente Lansingerland, Plan van aanpak Informatiebeveiliging, Overzicht van de verbeteracties 2015/2016, 28 november 2015.
[14] Gemeente Lansingerland, Plan van aanpak Informatiebeveiliging, Overzicht van de verbeteracties 2015/2016, 28 november 2015.
[15] Gemeente Lansingerland, 'Impactanalyse, resultaat na besluit; bijlage bij de GAP-analyse, 28 november 2015.
[16] In ambtelijk wederhoor is aangegeven dat "er met een frisse blik naar het tot en met 2015 opgehaalde materiaal gekeken is en er meer met een risico-analyseblik is gekeken naar de uit te voeren acties." Dit heeft volgens de gemeente geleid tot een iets andere opzet van de uit te voeren werkzaamheden. Voortschrijdend inzicht heeft volgens de gemeente gemaakt dat het plan van aanpak is bijgesteld. "De belangrijkste reden is dat in het oorspronkelijke plan nog niet was geëvalueerd welke maatregelen het meeste bijdragen aan de informatiebeveiliging en het snelste zijn te implementeren.

Het huidige plan van aanpak richt zich op de volgorde van de verschillende aspecten uit de BIG. Voor elke paragraaf uit de BIG is een separaat verbeterplan opgesteld. Deze plannen beschrijven de relevante dreigingen, de doelstelling en de te nemen maatregelen. De maatregelen worden op hoofdlijn weergegeven. Nadere operationalisatie, hoe de maatregelen moeten worden uitgevoerd of tussentijdse mijlpalen ontbreken. Het ontbreekt in deze plannen ook aan een planning en inzicht in de wijze waarop gemeten wordt of de implementatie van deze maatregelen op koers ligt. Wel wordt een verantwoordelijke benoemt die ervoor moet zorg dragen dat de maatregelen worden gerealiseerd. Dit zal gebeuren in de vorm van een werkgroep die de maatregelen nog nader moet uitwerken en invoeren.

nieuwe planning

In het informatiebeveiligingsplan werd de implementatie van de te nemen maatregelen uitgespreid over 2016 en 2017. In het meest recente plan van aanpak is deze planning losgelaten. De implementatie van maatregelen is planmatig over de hoofdstukken van de BIG, en in combinatie daarmee over het 2de, 3de en 4de kwartaal van 2016 verdeelt. De prioriteitstelling van de verschillende maatregelen is komen te vervallen. De rekenkamer merkt op dat dit een heel optimistisch tijdpad is. Sommige maatregelen, zoals het opstellen van een uitwisselingsbeleid en –procedures met derden en het waarborgen dat de dienstverlening door derden wordt nageleefd conform de beveiligingseisen en het aanpassen van de cultuur op de werkvloer, vergen in de ogen van de rekenkamer een langdurig proces. Er kan volgens de rekenkamer niet worden verwacht dat eind 2016 de beoogde maatregelen geheel zijn geïmplementeerd en op correcte wijze worden toegepast.
Het college heeft nergens aangegeven op welke termijn zij geheel wil voldoen aan de BIG. Het is niet inzichtelijk of de nieuwe planning nu nastreeft dat alle noodzakelijke maatregelen om te voldoen aan de BIG nu voor 2016 staan ingepland.[17] Dit lijkt wel zo te zijn, omdat nu ook maatregelen worden getroffen die niet eerder waren geprioriteerd.
Voor de invoering van de maatregelen ontbreekt een adequate planning. Ook is niet inzichtelijk op welke wijze het college de voortgang van de verbeteringen zal gaan monitoren, en hierop kan sturen. Daartoe zijn geen tussentijdse mijlpalen of expliciete monitoringsmomenten in de planning opgenomen. Het ontbreken van deze overkoepelende planning en een adequaat sturingsmechanisme leidt volgens de rekenkamer tot een hoog afbreukrisico.

bescherming persoonsgegevens

Naast de informatiebeveiliging heeft recent ook het gebruik van persoonsgegevens veel aandacht in de media gehad. Het gebruik van persoonsgegevens op het gebied van de Wet Bescherming Persoonsgegevens wordt door de gemeente niet als apart aandachtpunt meegenomen in haar verbeterplannen. Wel heeft de gemeente een inventarisatie naar de verwerking van persoonsgegevens laten uitvoeren.[18] Deze inventarisatie heeft echter de recente publicaties van de Autoriteit Persoonsgegevens

---

Op basis van de ervaringen van de externe projectleider zijn daarom een aantal onderdelen van het oorspronkelijke plan naar voren getrokken en andere naar achteren geplaatst." De rekenkamer merkt op dat de huidige indeling van verbetermaatregelen per achtereenvolgende paragraaf van de BIG is en daardoor juist de risicoanalyse niet meer van toepassing lijkt te zijn.

[17] Het is niet inzichtelijk gemaakt of de beschreven maatregelen in de verbeterplannen per aspect uit de BIG nu alle noodzakelijke maatregelen betreffen om aan de BIG te voldoen, of dat in de toekomst nog andere maatregelen noodzakelijk zijn.

[18] BMC advies, 'Persoonsinformatie en privacy. Op weg naar adequaat uitvoeringsniveau WBP door gemeente Lansingerland, 6 juni 2016.

niet meegenomen. Daarom heeft de rekenkamer gekeken naar de mate waarin de inventarisatie over de verwerking van persoonsgegevens (BMC-rapport), in combinatie met het register van de persoonsgegevens die worden verzameld, overeenstemt met de bevindingen van de Autoriteit Persoonsgegevens.
Het rapport van de Autoriteit Persoonsgegevens, 'Verwerking van persoonsgegevens in het sociaal domein: de rol van toestemming', geeft een bruikbare handleiding voor gemeenten over de wijze waarop gemeenten toestemming kunnen vragen voor het gebruik van persoonsgegevens, evenals de wijze van gebruik. Op basis van deze handleiding komt de rekenkamer tot vier aspecten die in gemeente Lansingerland, net als bij veel andere gemeenten[19], meer aandacht verdienen, te weten: de grondslag van de gegevensverzameling, het informeren van de burger, het domein overstijgend werken en daarbij vroeg signalering.

grondslag gegevensverzameling
Voor het verwerken van persoonsgegevens is een grondslag nodig. De mogelijke grondslagen zijn in de WBP verwerkt in artikel 8. De gemeente heeft een register aangelegd met daarin een inventarisatie van alle persoonsgegevens die door de gemeente verzameld worden. [20] In dit register staan onder het kopje rechtmatige grondslag verschillende wetten genoteerd als grondslag voor het verzamelen van deze gegevens. Dit zijn allerlei wettelijke bepalingen zoals de Jeugdwet, Burgerlijk Wetboek, Leerplichtwet en RMC-regeling. Deze toetsing is echter niet voldoende om aan de WBP gegevens te voldoen.[21] Voor de registratie van persoonsgegevens dient namelijk nog een toets plaats te vinden. De toets moet controleren of de desbetreffende wetgeving maakt dat er een wettelijke verplichting (artikel 8c WBP) of een publiekrechtelijke taak (artikel 8e WBP) is dat de gegevens verzameld worden, of dat er mogelijk een andere grondslag is om de gegevens te verzamelen. Hierbij moet ook geverifieerd worden of het ook bijzondere persoonsgegevens betreft, en of de gemeente wel een grondslag heeft om deze bijzondere persoonsgegevens te verzamelen (art. 16 t/m 24 WBP). Dit is in gemeente Lansingerland nog niet gebeurd. In ambtelijk wederhoor geeft gemeente Lansingerland aan dat deze toetsing wel heeft plaatsgevonden, maar dat deze niet expliciet is opgenomen in het register. Gelet op de bevinding van de rekenkamer zal gemeente Lansingerland dit expliciet in het register gaan vermelden, zo geeft de gemeente aan.[22]

informeren van de burger
De gemeente heeft ook de plicht de betrokkene te informeren over het registreren van zijn gegevens. Hierbij moet ook het doel van de informatieregistratie verteld worden. In de huidige registratietabel van gemeente Lansingerland is wel geïnventariseerd of er sprake is van vrijwaring, maar dit betreft de plicht de registratie te melden bij de Autoriteit Persoonsgegevens. Hierbij wordt dus nog niet ingegaan op de informatieplicht naar de burger. Bij deze informatieplicht is de wijze waarop dit informeren gebeurd ook van belang. Er kan niet naar een algemene tekst verwezen worden. Helemaal wanneer het bijzondere persoonsgegevens betreft, zoals bijvoorbeeld in het sociale domein. Er moet bij het verzamelen van persoonsgegevens onder meer verteld worden wat ermee wordt gedaan, met wie deze gegevens worden gedeeld en waarom. Bij de informatieplicht is het ook van

[19] Autoriteit persoonsgegevens, 'Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming', april 2016.
[20] Rekenkamer heeft deze ontvangen onder de naam Register Lansingerland.
[21] Autoriteit persoonsgegevens, 'Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming', april 2016.
[22] Gemeente Lansingerland, 'Reactie ambtelijk wederhoor', 7 september 2016.

belang dat gemeente Lansingerland de burgers zelf informeert indien de gemeente de persoonsgegevens van deze burger via iemand anders[23] ontvangt. In de verbeterplannen van gemeente Lansingerland wordt geen aandacht besteed aan het adequaat informeren van burgers. Evenmin is het onderdeel geweest van de inventarisatie die BMC[24] voor de gemeente heeft uitgevoerd over het gebruik van persoonsgegevens. In ambtelijk wederhoor wordt aangegeven dat gemeente Lansingerland wel aandacht besteed aan het informeren en het vragen van toestemming aan de burger. Dit is vastgelegd in de specifieke beleidsdocumenten. De rekenkamer heeft vervolgens enkele specifieke beleidsdocumenten geraadpleegd. Deze documenten besteden wel expliciet aandacht aan het gebruik van informatie maar niet aan de in de wet genoemde criteria waaraan het informeren van burgers moet voldoen.

domein overstijgend werken

Bij de verschillende taken van de gemeente in het sociaal domein is het gebruikelijk om domein overstijgend te werken. Voorbeeld hiervan is samenwerken met organisaties in de (jeugd)zorg. Hieraan zit echter een aantal haken en ogen. Domein overstijgend werken is niet vastgelegd als werkwijze in de desbetreffende wetgeving (de materiewetten). Deze werkwijze kan daardoor niet gezien worden als de directe uitoefening van een publiekrechtelijke taak.[25] Verzamelde persoonsgegevens kunnen dan ook niet voor dit domein overstijgende werkzaamheden gebruikt worden. In de inventarisatie[26] die gemeente Lansingerland heeft laten uitvoeren, wordt aangegeven dat bij de uitvoering van deze taken met toestemming van de burger gewerkt kan worden. De rekenkamer merkt op, in lijn met het rapport van de Autoriteit Persoonsgegevens, dat de gemeente er in dit geval rekening mee moet houden dat er beperkingen zitten aan het gebruik van toestemming. Bij het vragen van toestemming moet de betrokkene namelijk geheel vrij zijn nee te kunnen zeggen. Indien het verkrijgen van hulp (voor het gevoel van de burger) afhangt van deze toestemming, is het geven van toestemming niet geheel vrij. Het geven van toestemming door de burger is in deze gevallen niet voldoende.[27] Er moet in deze gevallen gekeken worden of er een andere grondslag is voor het delen van de gegevens. Dit heeft gemeente Lansingerland nog niet gedaan. Daarnaast is ook van belang dat als gegevens worden verzameld door een hulpverlener, deze hulpverlener deze gegevens niet zomaar mag delen. Hulpverleners hebben namelijk vaak een beroepsgeheim. Naast een grondslag uit de WBP om gegevens te mogen delen moet er in dit geval ook een grond zijn voor het doorbreken van het beroepsgeheim.

vroeg signalering

Er bestaan verschillende vormen van vroeg signalering. Een deel van deze vormen van vroeg signalering is niet wettelijk geregeld, zoals het registreren van signalen en meldingen van bezorgde professionele hulpverleners of anderen. Ook domein overstijgende vroeg signalering is niet wettelijk geregeld. Vroeg signalering zoals die

---

[23] Dit kan een andere organisatie zijn.
[24] BMC advies, 'Persoonsinformatie en privacy. Op weg naar adequaat uitvoeringsniveau WBP door gemeente Lansingerland, 6 juni 2016.
[25] Autoriteit persoonsgegevens, 'Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming', april 2016.
[26] BMC advies, Persoonsinformatie en privacy. Op weg naar adequaat uitvoeringsniveau WBP door gemeente Lansingerland, 6 juni 2016.
[27] Autoriteit persoonsgegevens, 'Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming', april 2016.

binnen het sociaal domein nu vorm krijgt, is daardoor geen publiekrechtelijke taak.[28] Dit maakt dat artikel 8c WBP geen grondslag is voor het registreren van gegevens te verzamelen over burgers of gezinnen in een stadium waarin betrokkenen zelf (nog) niet om hulp of ondersteuning vragen. Indien de gemeente dit wel doet moet er daarom een andere grondslag voor het verzamelen van deze gegevens gevonden worden. In gemeente Lansingerland wordt gewerkt met vroeg signalering, maar ontbreekt, landelijk, een correcte wettelijke grondslag.

reactie college

Op 16 september 2016 ontvingen wij uw notiebrief informatiebeveiliging. Wij waarderen het zeer dat u met deze brief enkele aanbevelingen doet die de gemeente Lansingerland kan gebruiken om de informatiebeveiliging verder te ontwikkelen. Wij zullen deze aanbevelingen dan ook zeker betrekken bij de verdere implementatie van de BIG. Wij vinden het wel jammer dat de algemene teneur van de brief is dat de gemeente onvoldoende actie lijkt te ondernemen c.q. het college het belang van informatiebeveiliging en de daarin te nemen stappen onderschat. Dit doet ons inziens geen recht aan de stappen die reeds zijn gemaakt en de dagelijkse aandacht die voor dit thema is binnen onze organisatie. Hierna geven wij voor de belangrijkste bevindingen uit de brief onze bestuurlijke reactie weer.

Visie op informatiebeveiliging

U geeft in uw brief aan dat u een visie van de gemeente Lansingerland op informatiebeveiliging mist. Op 6 september jl. is aan de raad de presentatie gegeven "I&A op weg naar 2020". Deze presentatie geeft een brede visie op ons informatiebeleid. Informatiebeveiliging is hierin benoemd als één van de belangrijkste speerpunten. Een volledige visie op dit speerpunt zullen wij na het vaststellen van het informatiebeleid verder uitwerken.

Informatiebeveiligingsbeleid en beveiligingsplan: planning en monitoren voortgang

Uw bevindingen ten aanzien van de planning en het monitoren van de voortgang herkennen wij. U vat dit zelf kort en krachtig samen in de laatste alinea onder het kopje ‘nieuwe planning’. Inmiddels zijn afspraken gemaakt met de externe projectleider en de informatiebeveiligingsfunctionaris om de overkoepelende planning inclusief mijlpalen te actualiseren en daarmee ook de stuurgroep informatiebeveiliging en het college periodiek te informeren over de voortgang van de implementatie.

Overigens betekent het ontbreken van actueel inzicht in de planning en voortgang niet dat er de afgelopen maanden geen voortgang is geboekt. Die voortgang is er wel degelijk. Zo zijn van de 42 direct te implementeren maatregelen inmiddels 23 geïmplementeerd, zijn 9 van deze maatregelen onderdeel van de nieuwe bewustwordingscampagne (die in oktober 2016 van start gaat) en hebben 5 maatregelen betrekking op het op papier zetten van procedures. Het beschrijven hiervan vindt momenteel plaats.

Uw brief bevat een aantal passages die niet (concreet) onderbouwd zijn

Een aantal passages in uw brief zijn naar onze mening niet (concreet) onderbouwd en sluiten niet geheel aan bij de feitelijke gang van zaken of standpunten van het college. Het gaat dan vooral om de volgende passages:

[28] Autoriteit persoonsgegevens, ‘Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming’, april 2016.

- Blz. 1, 1e alinea. ‘Dit beeld wordt bevestigd door recent onderzoek door internet.nl naar de beveiliging van gemeentelijke websites’. Dit onderzoek staat volledig los van de eerder in de brief aangehaalde digitale toegang tot data. Daar komt bij dat het onderzoek van internet.nl zich beperkte tot een bepaald onderdeel van onze website. Wij verwijzen o.a. naar de, door u zelf aangehaalde brief, die het college aan de Raad zond over dit onderwerp. De Rekenkamer verwijst hier naar een onderzoek van internet.nl zonder dat zij zelf kennis heeft genomen van dit onderzoek en vastgesteld heeft dat dit een deugdelijk onderzoek is geweest.

- Blz. 3, 2e alinea. ‘Naar de mening van de Rekenkamer laat de risico-inventarisatie zien dat nog relatief grote inspanningen moeten worden verricht om te komen tot de beoogde resultaten. Dit lijkt het college soms te onderschatten. In het beveiligingsplan wordt bijvoorbeeld aangegeven dat de categorie mensen (in relatie tot onder meer naleving) aandacht verdient, omdat met relatief weinig inspanning een groot effect kan worden behaald. De Rekenkamer is van mening dat de gemeente de benodigde inspanningen voor een cultuur- en gedragsverandering onderschat.’ Ambtelijk en op collegeniveau onderschatten we de inspanningen zeker niet. U refereert hier ook aan in uw voetnoot bij deze passage. Komend najaar start een campagne om informatiebeveiliging hernieuwd gemeente breed onder de aandacht te brengen en de komende jaren ook te houden. In 2012/2013 zijn al door een extern bureau bewustwordingssessies gehouden voor afdelingshoofden en teamleiders. Tenslotte merken wij op dat de noodzakelijk te maken stappen naast cultuur, houding en gedrag ook betrekking hebben op het volledig op orde hebben van de organisatorische, technische en procedurele kant van informatiebeveiliging. Zonder dat deze ‘basis’ op orde is, is het bewust maken van de organisatie namelijk ook minder effectief.

Bescherming persoonsgegevens
Voor dit onderdeel van de brief heeft u aansluiting gezocht bij de publicatie van de Autoriteit
Persoonsgegevens en benoemt vier aspecten die bij landelijk en dus ook bij onze gemeente meer aandacht verdienen. Samengevat zijn deze aspecten terug te voeren naar het informeren van burgers over het verwerken van persoonsgegevens (welke gegevens en met wel doel) en de ‘uitdrukkelijke’ toestemming die burgers moeten geven voor het verwerken van deze (bijzondere) persoonsgegevens.

Informeren van de burger en verkrijgen van toestemming
In uw brief staat dat In de verbeterplannen van de gemeente Lansingerland geen aandacht wordt besteed aan het adequaat informeren van de burgers. Binnen het Sociaal Domein vragen wij in Lansingerland wel degelijk toestemming aan betrokkenen en informeren hen daarbij ook met welk doel gegevens worden verwerkt. Dit is vastgelegd in beleidsdocumenten, protocollen en werkinstructies. Die protocollen zijn ook afgestemd met de Adviesraad Sociaal domein (of haar voorgangers). Zo wordt met betrokkenen besproken en vastgelegd of zij toestemming geven. Wanneer betrokkenen geen toestemming willen geven, dan wordt de informatie niet gedeeld. Dit betekent echter niet dat er geen dienstverlening plaatsvindt. Eventuele derden dienen de informatie dan bij de klant zelf op te vragen. Burgers met multi-problematiek worden besproken in de Commissie Sluitende Aanpak Volwassenen (CSAV). De betrokken zorgverlener zal hiervoor eerst toestemming vragen aan de cliënt, mondeling of middels het invullen van het toestemmingsformulier. In enkele gevallen worden casussen zonder toestemming besproken maar dan zijn de gegevens anoniem. Dat in de beleidsdocumenten

wellicht niet expliciete aandacht wordt besteed aan de in de wet genoemde criteria, betekent derhalve niet dat burgers niet adequaat worden geïnformeerd.

Domein overstijgend werken
U geeft aan dat indien het verkrijgen van hulp (voor het gevoel van de burger) afhangt van de toestemming om gegevens te verwerken, het geven van de toestemming niet geheel vrij is. En dat In deze gevallen moet bekeken worden of er een andere grondslag is voor het delen van de gegevens. U geeft aan dat de gemeente Lansingerland dit nog niet gedaan heeft. Dit algemene uitgangspunt is juist, maar er is door u niet aangegeven op welke specifieke situaties bij Lansingerland u dan doelt of dat u alleen het algemene landelijke uitgangspunt beschrijft (dus niet iets specifiek voor Lansingerland).

Vroeg signalering
Onder vroeg signalering geeft u terecht aan dat domein overstijgende vroeg signalering niet wettelijk is geregeld en daardoor geen publiekrechtelijke taak is. Hierdoor is artikel 8c Wbp geen grondslag voor het registreren van persoonsgegevens. Uw conclusie dat wanneer een gemeente dit wel doet, zoals in Lansingerland, er een correcte wettelijke grondslag ontbreekt is dus niet iets specifiek voor Lansingerland. Wel zullen wij, gelet op uw advies, een protocol opstellen met betrekking tot vroeg signalering.

Nawoord rekenkamer
De rekenkamer is blij met de constructieve reactie van het college en de toezegging om de aanbevelingen te betrekken bij de implementatie van de BIG. Voorts wil de rekenkamer opmerken dat zij nog geen onderzoek heeft uitgevoerd naar de informatiebeveiliging in Lansingerland. Op basis van de verzamelde informatie voor het schrijven van een onderzoeksopzet concludeerde de rekenkamer dat het college momenteel met een omvangrijk traject is gestart om de informatiebeveiliging op peil te brengen. Op basis van de aangeleverde documentatie voor het schrijven van een onderzoeksopzet is de rekenkamer op basis van eerste bevindingen tot een aantal noties gekomen, zoals weergegeven in de notiebrief.

De rekenkamer is niet van mening dat het college onvoldoende actie onderneemt op het gebied van informatiebeveiliging. In de notiebrief wordt juist aangegeven dat op dit moment veel activiteiten worden ondernomen om de beveiliging te verbeteren. Wel is de rekenkamer van mening dat het college de benodigde implementatietijd en de hoeveelheid inspanningen die het kost om een cultuur te veranderen onderschat. In het afgelopen half jaar zijn 23 van de 42 meest door de gemeente noodzakelijk geachte maatregelen geïmplementeerd. Dit waren maatregelen die volgens de gemeente ook met relatief weinig inspanning snel konden worden gerealiseerd. De resterende maatregelen (waaronder het beschrijven van procedures en het bewustmaken van gebruikers) moeten nog worden ingevoerd. Daarnaast zijn nog veel meer maatregelen (157) nodig om aan de BIG te voldoen. Om dit binnen de tijdspanne van 2016 en mogelijk 2017 te kunnen realiseren lijkt de rekenkamer zeer optimistisch.

Dat de gemeente een volledige visie op informatiebeveiliging gaat uitwerken, juicht de rekenkamer toe. Eenzelfde geldt voor de bewustwordingssessies. Om het bewustzijn blijvend te versterken, zal over langere termijn aandacht voor het onderwerp moeten worden gevraagd.

Voor wat betreft de bescherming van persoonsgegevens constateert de rekenkamer dat de gemeente inderdaad vraagt aan de burger of zij al dan niet toestemming willen verlenen. Echter, wanneer een burger om zorg vraagt, kan deze zich zonder dit te benoemen toch gedwongen voelen om positief te antwoorden. Dit uit angst voor zijn omstandigheden of uit angst om anders geen zorg te krijgen. Er moet sprake zijn van vrije toestemming. Vrije toestemming houdt in dat de betrokkene zich niet verplicht voelt om toestemming te geven vanwege druk van de omstandigheden waarin hij verkeert of de relatie waarin hij tot de verantwoordelijke staat.[29] Vanuit dit perspectief moet, zo geeft de Autoriteit bescherming persoonsgegevens aan, de burger ook geïnformeerd worden over de criteria die in de wet zijn benoemd (zoals het doel waarom de gegevens worden geregistreerd en mogelijk gedeeld, het specificeren van partijen, welke gegevens worden uitgewisseld etc.). Dit is inderdaad in veel gemeenten het geval en zo ook in Lansingerland. Rekenkamer Lansingerland beveelt de gemeente aan om expliciet gebruik te maken van de handleiding die de Autoriteit bescherming persoonsgegevens heeft opgesteld, om na implementatie van alle verbetermaatregelen door de gemeente ook op dit aspect aan de wet te kunnen voldoen.

Met vriendelijke groet,

drs. P Hofstra RO CIA
directeur Rekenkamer Lansingerland

[29] Autoriteit persoonsgegevens, 'Verwerking van persoonsgegevens in het sociaal domein: De rol van toestemming', april 2016.