Rekenkamer
LANSINGERLAND

informatiebeveiliging

juli 2017

Rekenkamer LANSINGERLAND

1 inleiding

1-1 aanleiding

Gemeenten hebben als gevolg van de decentralisaties in het sociaal domein steeds meer (bijzondere) persoonsgegevens[1] in beheer. Ook wordt steeds meer informatie digitaal opgeslagen en overgedragen en worden systemen en data steeds vaker aan elkaar gekoppeld. Het belang van gemeenten om de informatiebeveiliging op orde te hebben en weerbaar te zijn tegen dreigingen als cybercrime is als gevolg van deze ontwikkelingen aanzienlijk toegenomen. Het belang van dit onderwerp bleek ook uit de uitslag van de stemkastsessie op 9 december 2015 met de gemeenteraad, waarbij het onderwerp informatiebeveiliging als zeer relevant werd benoemd.

De Rekenkamer Lansingerland heeft op 15 december 2015 aangegeven een onderzoek te willen starten naar de informatiebeveiliging in de gemeente Lansingerland. Naar later bleek was de timing van dit onderzoek naar informatiebeveiliging niet ideaal, zoals vervolgens is aangegeven in een brief van 25 mei 2016[2] aan de raad. Dit had er mee te maken dat binnen de gemeente Lansingerland veel ontwikkelingen gaande waren op het gebied van informatiebeveiliging.

De Rekenkamer Lansingerland heeft daarom besloten om het onderzoek naar informatiebeveiliging op een later moment voort te zetten. Wel heeft de rekenkamer door middel van een tussentijdse rapportage[3] de eerste bevindingen van haar onderzoek gedeeld met de raad.

In de onderzoeksprogrammering voor 2017 heeft de rekenkamer aangegeven in 2017 het eerder geplande onderzoek uit te voeren. In deze onderzoeksopzet licht de rekenkamer toe hoe invulling zal worden gegeven aan dit onderzoek.

1-2 leeswijzer

Paragraaf 2 licht de beleidsmatige, juridische en organisatorische context van het onderzoek toe. Aansluitend komen in paragraaf 3 de doel- en vraagstelling en de afbakening van het onderzoek aan de orde. In paragraaf 4 wordt de onderzoeksaanpak beschreven en tot slot komt in paragraaf 5 de planning en organisatie van het onderzoek aan de orde.

1 Een persoonsgegeven is iedere vorm van informatie die direct over iemand gaat of naar deze persoon te herleiden is. Bij bijzondere persoonsgegevens gaat het om informatie over iemands godsdienst of levensovertuiging, ras, politieke voorkeur, gezondheid, seksuele leven, lidmaatschap van een vakbond of strafrechtelijk verleden. Bijzondere persoonsgegevens mogen niet gebruikt worden, tenzij daarvoor een wettelijke uitzondering geldt. Bron: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/persoonsgegevens/wat-zijn-persoonsgegeven.

2 Rekenkamer Lansingerland, brief aan de gemeenteraad van Lansingerland ‘voortgang onderzoeksprogramma 2016’, 25 mei 2016.

3 Rekenkamer Lansingerland, brief aan de gemeenteraad van Lansingerland ‘notiebrief informatiebeveiliging’, 3 oktober 2016.

2 context

2-1 informatiebeveiligingsbeleid

Kortheidshalve zal het informatiebeveiligingsbeleid op deze plek alleen op hoofdlijnen worden beschreven. De in de inleiding genoemde tussentijdse rapportage van de rekenkamer bevat een meer uitgebreide beschrijving van het beleid.

De gemeente Lansingerland heeft een door het college van B en W vastgesteld informatiebeveiligingsbeleid.[4] De indeling van het beleidsplan is gebaseerd op de Baseline Informatiebeveiliging Gemeenten (BIG), een door de Vereniging Nederlandse Gemeenten (VNG) opgestelde beschrijving van de wijze waarop gemeenten de veiligheid van informatie conform internationale standaarden voor informatiebeveiliging kunnen borgen. Gemeenten zijn niet verplicht de BIG in te voeren, wel heeft de algemene ledenvergadering van de VNG zich gecommitteerd aan de invoering van de BIG.[5] Per onderdeel van de BIG worden in het informatiebeveiligingsbeleid een algemene doelstelling, het beoogde resultaat en de basisnormen beschreven. Tevens is in het beleid de organisatie van de informatiebeveiliging beschreven.

Op basis van het informatiebeveiligingsbeleid is in november 2015 een informatiebeveiligingsplan[6] opgesteld. 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. Hierbij waren 42 van de 204 nog te implementeren maatregelen uit de BIG geprioriteerd. Tevens bevat het plan een planning van verbetermaatregelen. In zijn tussentijdse rapportage heeft de rekenkamer opgemerkt dat deze planning erg optimistisch is en het niet duidelijk is of, en zo ja wanneer de gemeente beoogd te voldoen aan alle eisen van het BIG. In een presentatie aan de gemeenteraad, gehouden op 31 januari 2017, is de toenmalige stand van zaken ten aanzien van de implementatie toegelicht. Op dat moment waren de 42 maatregelen met prioriteit nog niet volledig geïmplementeerd. Uit een interne notitie van de gemeente blijkt dat de gemeente in mei 2017 voldoet aan 57% van de maatregelen uit de BIG.[7]

2-2 juridische context

Wet bescherming persoonsgegevens

De Wet bescherming persoonsgegevens (Wbp) is de Nederlandse uitwerking van de Europese richtlijn bescherming persoonsgegevens.[8] In artikel 13 Wbp is bepaald dat sprake moet zijn van passende technische en organisatorische maatregelen om persoonsgegevens te beveiligen tegen verlies of onrechtmatige verwerking. Er moet sprake zijn van een passend beveiligingsniveau, gelet op de risico's die de verwerking

4 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015.

5 VNG, resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente', aangenomen op 29 november 2013.

6 Gemeente Lansingerland, 'Informatiebeveiligingsplan', 28 november 2015

7 Gemeente Lansingerland, Informatieveiligheidsanalyse Mei 2017, juni 2017.

8 Op Europees niveau is overeenstemming bereikt over de algemene verordening inzake gegevensbescherming. Deze verordening moet o.a. leiden tot een betere bescherming van gegevens van burgers. De verordening zal in 2018, na een overgangsperiode van twee jaar, van kracht worden.

en de aard van de te beschermen gegevens met zich meebrengen. Door een wijziging van de Wbp kan de Autoriteit Persoonsgegevens gemeenten vanaf 1 januari 2016 ook boetes opleggen bij overtreding van de wet. Tevens moeten gemeenten vanaf 1 januari 2016, wanneer sprake is van een inbreuk op de beveiliging van persoonsgegevens (een 'datalek'), direct een melding doen bij de Autoriteit Persoonsgegevens. Een datalek kan bijvoorbeeld een hack van een bestand of het verlies van een USB-stick met persoonsgegevens zijn.

Het gebruik van persoonsgegevens op het gebied van Wbp wordt door de gemeente niet als apart aandachtspunt meegenomen in haar verbeterplannen, terwijl dit voor de hand ligt gezien de decentralisaties in het sociaal domein en het risico op datalekken en boetes. Wel is in 2016 een inventarisatie uitgevoerd door een extern adviesbureau naar de verwerking van persoonsgegevens.[9] Mede op grond van deze inventarisatie identificeerde de rekenkamer in haar tussentijdse rapport vier aspecten van persoonsgegevensbeheer die in gemeente Lansingerland, net als bij veel andere gemeenten, meer aandacht verdienen, te weten: de grondslag van de gegevensverzameling, het informeren van de burger, het domein overstijgend werken en daarbij vroeg signalering.

Wet basisregistratie personen
De verwerking van persoonsgegevens uit de basisregistratie personen valt niet onder de Wbp. Voor deze gegevens zijn de regels voor het gebruik en de beveiliging vastgelegd in de Wet basisregistratie personen (Wet BRP). In artikel 6 lid 1 van het besluit basisregistratie personen staat dat het college van B en W maatregelen moet treffen om de gegevens uit de basisregistratie personen te beveiligen. Deze maatregelen zijn beschreven in de beheerregeling gemeentelijke basisregistratie persoonsgegevens voor de gemeente Lansingerland 2012.

2-3 organisatorische context

Het college van B en W draagt de integrale verantwoordelijkheid voor de beveiliging van informatie binnen de werkprocessen van de gemeente. Binnen de ambtelijke organisatie zijn de verantwoordelijkheden voor informatiebeveiliging verdeeld over de volgende functies:

- De gemeentesecretaris is gemandateerd verantwoordelijk voor informatiebeveiliging.
- De Chief Information Security Officer (CISO) is op organisatieniveau verantwoordelijk voor het actueel houden van het beleid, het adviseren bij projecten en het managen van risico's evenals het opstellen van rapportages. Sinds 1 juni 2016 is deze functie vacant.
- De controller informatiebeveiliging is op organisatieniveau verantwoordelijk voor de verbijzonderde interne controle op de naleving van het informatiebeveiligingsbeleid, de controle op de realisatie van voorgenomen veiligheidsmaatregelen en de escalatie van beveiligingsincidenten.
- De beveiligingsfunctionarissen rijbewijzen en reisdocumenten zijn verantwoordelijk voor toezicht op de naleving van de beveiligingsprocedures rond deze documenten.

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

- De afdelingshoofden zijn verantwoordelijk voor de (informatie)veiligheid en de betrouwbaarheid van de informatieprocessen en systemen binnen hun afdeling.[10]

3 doel- en vraagstelling

3-1 doelstelling

De rekenkamer beoogt met dit onderzoek na te gaan of (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Lansingerland in veilige handen zijn.

3-2 vraagstelling

De centrale vraag van het onderzoek luidt als volgt:

De centrale onderzoeksvraag luidt als volgt:
Zijn (bijzondere) persoonsgegevens en andere gevoelige informatie bij de gemeente Lansingerland in veilige handen?

De centrale onderzoeksvraag is uitgewerkt in de volgende deelvragen:

1 Heeft de gemeente Lansingerland in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?
2 Heeft de gemeente Lansingerland adequate maatregelen getroffen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's?
3 Is het mogelijk om oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens en andere gevoelige informatie die de gemeente Lansingerland in beheer heeft? En zo ja, welke gevolgen kan dit hebben voor burgers?

3-3 afbakening

Met betrekking tot de afbakening van dit onderzoek zijn de volgende punten relevant:

- In het kader van deelvraag 1 beoogt de rekenkamer na te gaan of de gemeente de belangrijkste risico's (met in potentie de grootste impact) in beeld heeft. De rekenkamer zal dus niet beoordelen of de gemeente alle potentiële risico's in beeld heeft.
- In het kader van deelvraag 2 kijkt de rekenkamer zowel naar maatregelen die op niveau van het concern worden getroffen, als maatregelen binnen de individuele afdelingen. Daarbij neemt de rekenkamer zowel technische als organisatorische (o.a. gericht op de beheersing van het gedrag van medewerkers) beveiligingsmaatregelen in ogenschouw. De rekenkamer beperkt zich hierbij tot de beveiligingsmaatregelen voor (bijzondere) persoonsgegevens die de gemeente beheert als gevolg van de decentralisaties in het sociaal domein.
- In het kader van deelvraag 3 zal de rekenkamer testen of het mogelijk is oneigenlijke toegang te krijgen tot (bijzondere) persoonsgegevens

10 College van B en W, 'Gemeente breed informatiebeveiligingsbeleid', vastgesteld op 26 mei 2015.

en andere gevoelige informatie die de gemeente in beheer heeft als gevolg van decentralisaties in het sociaal domein. Door een penetratietest worden de technische beveiligingsmaatregelen van ICT-systemen getest. Een zogeheten 'social engineering' test richt zich op de menselijke kant van de beveiliging; het veiligheidsbewustzijn van medewerkers. Door de social engineering test te herhalen zal getracht worden een zo betrouwbaar mogelijk beeld van dit onderdeel van de beveiliging te verkrijgen.

4 onderzoeksaanpak

4-1 documentstudie en interviews

In het kader van dit onderzoek zal de rekenkamer o.a. de volgende documenten bestuderen:
• beleidsstukken, regelingen, procedures e.d. ten aanzien van de informatiebeveiliging en het beheer van (bijzondere)persoonsgegevens;
• voortgangs- en auditrapportages m.b.t. informatiebeveiliging en het beheer van (bijzondere)persoonsgegevens;
• risico- en/of dreigingsanalyses;
• documenten m.b.t. informatiebeveiliging en het beheer van (bijzondere) persoonsgegevens.

In het kader van dit onderzoek zullen interviews worden gehouden met:
• de gemeentesecretaris, CISO en controller informatiebeveiliging of degenen die de bij deze functies behorende werkzaamheden in de praktijk uitvoeren;
• ambtenaren die verantwoordelijk zijn voor informatiebeveiliging of taken uitvoeren op dit gebied.

4-2 testen mogelijkheden oneigenlijke toegang

De rekenkamer zal voor de uitvoering van dit onderzoek externe deskundigheid inhuren van een bedrijf met expertise op het gebied van informatiebeveiliging en bescherming van (bijzondere) persoonsgegevens en de specifieke kennis om te testen of het mogelijk is oneigenlijke toegang te krijgen tot deze gegevens. Dit bedrijf mag geen opdrachten op het gebied van informatiebeveiliging hebben uitgevoerd voor de gemeente Lansingerland.

Voor de beantwoording van deelvraag 3 laat de rekenkamer een zogeheten penetratietest uitvoeren. Deze test kan bestaan uit:
- Het van buitenaf binnendringen in de informatiesystemen van de gemeente.
- Het van binnenuit, met een reguliere gebruikersaccount, proberen toegang te krijgen tot systemen waarvoor geen rechten zijn verleend. Het gaat hierbij om systemen met veel gevoelige (persoons)gegevens, die worden gebruikt in het sociaal domein. Tevens zal onderzocht worden of het mogelijk is om oneigenlijk toegang te krijgen tot specifieke agenda's, e-mails, bestanden of dossiers.

Naast de penetratietest, zal ook een 'social engineering' test worden uitgevoerd. Onderdeel van deze test kunnen zijn:
- het versturen van phishing e-mails met een bijlage met malware;

- het verspreiden van usb-sticks die, wanneer zij gebruikt worden, malware installeren;
- via de telefoon of e-mail verzoeken om vertrouwelijke gegevens te delen;
- een inlooptest, waarbij mystery guests locaties proberen te betreden waartoe zij eigenlijk geen toegang hebben.

De daadwerkelijke uitvoering gebeurt na overleg met de gemeentelijke organisatie, waarbij voorafgaand een vrijwaringsovereenkomst zal worden getekend tussen de gemeente, het onderzoeksbureau en de Rekenkamer Lansingerland. De rekenkamer zal voor dit deel van het onderzoek geen onderzoekswerkzaamheden (laten) uitvoeren zonder medeweten van de gemeente. Er zal voor worden gewaakt dat door de tests schade ontstaat of bedrijfsprocessen worden verstoord. Wanneer ambtenaren onbedoeld oneigenlijk toegang of informatie verschaffen zal slechts worden geregistreerd dat dit gebeurt en niet door wie. Grote en urgente beveiligingsrisico's zullen direct worden gecommuniceerd aan de voor informatiebeveiliging verantwoordelijke ambtenaren.

Bij de beantwoording van onderzoeksvraag 2 en 3 zal de rekenkamer ook de uitkomsten van door de gemeente uitgevoerde beveiligingstesten, zelfassessments en audits betrekken.

4-3 normenkader

In tabel 4-1 is het globale normenkader opgenomen dat de rekenkamer in dit onderzoek zal hanteren voor de deelvragen 1 en 2. Gezien de aard van deelvraag 3 worden bij die onderzoeksvraag geen normen gehanteerd. Het normenkader zal in overleg met de externe deskundigen die voor dit onderzoek worden ingehuurd, nader worden gespecificeerd.

tabel 4-1: normenkader

deelvraag	norm
1 Heeft de gemeente Lansingerland in brede zin een goed beeld van de belangrijkste risico's op het gebied van informatiebeveiliging en in het bijzonder de bescherming van (bijzondere) persoonsgegevens en andere gevoelige informatie?	• Op concernniveau en binnen de individuele afdelingen worden met voldoende frequentie risicoanalyses en/of dreigingsanalyses gemaakt. • In de risicoanalyses en/of dreigingsanalyses zijn de belangrijkste risico's geïdentificeerd. • De risicoanalyses en/of dreigingsanalyses geven inzicht in specifieke risico's m.b.t. het beheer van (bijzondere) persoonsgegevens.
2 Heeft de gemeente Lansingerland adequate maatregelen getroffen om de (bijzondere) persoonsgegevens en andere gevoelige informatie die zij in beheer heeft te beschermen tegen de belangrijkste veiligheidsrisico's?	• De maatregelen sluiten aan op de risico's die zijn geïdentificeerd. • De gemeente heeft technische maatregelen getroffen die de risico's doen afnemen. • De gemeente heeft organisatorische maatregelen getroffen die de risico's doen afnemen.

5 organisatie en planning

5-1 organisatie

Het onderzoek zal worden uitgevoerd door een onderzoeksteam van de Rekenkamer Lansingerland, bestaande uit:

- de heer Laurens Wijmenga (projectleider);
- mevrouw Rosa Ridderhof (onderzoeker);
- mevrouw Yiman Fung (senior onderzoeker).

5-2 planning

De uitvoering van dit onderzoek start in juli 2017. De penetratietest en social engineering test zullen naar verwachting worden verricht in september. Publicatie van het rapport is voorzien in het najaar van 2017.