Rekenkamercommissie

Onderzoek naar informatiebeveiliging en datalekken

---

1 aanleiding

Gezien de maatschappelijke taak die gemeentes hebben verwerken gemeenten, zowel digitaal als analoog, persoonsgegevens. Door verschillende ontwikkelingen, zoals de decentralisaties in het sociaal domein, zijn die persoonsgegevens steeds meer vertrouwelijk van aard. De afgelopen tijd is de regelgeving voor het verwerken van persoonsgegevens aangescherpt. Zo ook op het gebied van de Informatieveiligheid waar bijvoorbeeld de Wet op de datalekken onlangs in werking is getreden. In het kader van informatieveiligheid zijn er voor gemeenten nieuwe verplichtingen ontstaan over de wijze waarop zij de verwerking van persoonsgegevens beveiligen. Dit brengt voor gemeenten ook nieuwe "rollen" met zich mee, met betrekking tot die informatieveiligheid, zoels het aanstellen van een CISO en een privacy-officer en er zijn nieuwe verplichtingen zoals de ENSIA (Eenduidige Normatiek Single Information Audit). Die nieuwe verplichtingen en nieuwe rollen hebben tot doel om het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control -cyclus (waarmee consistente sturing beoogd wordt).

Het toenemende verwerking van (gevoelige) persoonsgegevens, de toename in technologie en de wijzigingen van de verplichtingen op dit gebied brengen potentiële risico's (m.n. financieel en politiek) met zich mee. Rondom dit thema ziet de rekenkamercommissie aanleiding te onderzoeken hoe het vraagstuk van informatiebeveiliging binnen de vier gemeenten is georganiseerd om er zo voor te zorgen dat de gemeenten inzicht krijgen in de veiligheid van de manier waarop zij persoonsgegevens verwerken.

Dit is het eerste onderzoek waarmee voor de vier gemeenten gezamenlijk één onderzoeksonderwerp wordt opgepakt. Hiermee geven wij invulling aan de wens die vanuit de gemeenteraden is geuit om de synergie voordelen van één rekenkamercommissie voor vier gemeenten te benutten. Het onderzoek geeft namelijk de mogelijkheid voor een onderlinge vergelijking waarmee de gemeenten voordeel kunnen doen.

2 afbakening

Deze overwegingen leiden tot de volgende set aan hoofd- en deelvragen:

2.1 Hoofdvraag.

In hoeverre voldoet de wijze waarop de gemeenten Meppel, Staphorst, Steenwijkerland en Westerveld de verwerking van persoonsgegevens beveiligen aan de (gestelde) vereisten op wettelijk en technologische gebied?

Ter beantwoording van deze hoofvraag zijn de volgende deelvragen geformuleerd.

2.2 Deelvragen.

Om de hoofdvraag verder uit te werken in deelvragen, stellen we vragen over de organisatie, mensen en gedrag en de techniek. Hieronder presenteren we deze deelvragen van het onderzoek

Organisatie en beleid
Is er gemeentelijk beleid op het gebied van informatiebeveiliging?
Startpunt van het onderzoek vormt het gemeentelijke beleid. Daarin zullen overigens de wettelijke vereisten als basis en vertrekpunt een rol moeten spelen.

Worden er systematische en actuele risocoanalyses gemaakt rond informatiebeveiliging en worden er op basis daarvan passende beheersmaatregelen genomen?
Bij deze analyses denken we onder andere aan het beheer van ICT-middelen, cryptografie, toegangsbeveiliging, fysieke beveiliging, leveranciersmanagement, beheer van informatie-beveiligingsincidenten (datalekken) en Back-up & Disaster Recovery.

Biedt het informatiebeveiligingsbeleid voldoende basis voor de bescherming van gegevens?
De basis van informatiebeveiligingsbeleid kan gevonden worden in diverse standaarden en regelingen (BIG, ISO2001:2013, AVG). De gemeente beheert daarbij een aantal gevoelige systemen (GBA, uitkeringen, DiGiD, WMO, ..). Het is belangrijk dat het infomatiebeveiligingsbeleid juist met deze systemen rekening houdt.

Is het informatiebeveiligingsbeleid vertaald naar concrete activiteiten en zijn hiervoor voldoende middelen beschikbaar gesteld?

Zijn binnen de organisatie de rollen en verantwoordelijkheden voor informatiebeveiliging helder belegd?

Wordt de Raad periodiek geïnformeerd over de status van informatiebeveiliging?

Mens en gedrag
Het tweede element in het geheel van informatiebeveiliging is mens en gedrag. Daarover stellen we de volgende vragen:

Is het hogere management actief betrokken bij informatiebeveiliging en het uitdragen daarvan binnen de organisatie?
Het hogere management vervult een belangrijke voorbeeldfunctie, bijvoorbeeld door de wijze waarop invulling wordt gegeven aan de rollen en verantwoordelijkheden.

Zijn medewerkers bewust van informatiebeveiligingsrisico's en is voor medewerkers duidelijk wat van hun verwacht wordt ten aanzien van informatiebeveiliging?
Het is belangrijk dat er een breder bewustzijn binnen de organisatie is van het belang van informatie-beveiliging en de wijze waarop medewerkers daarin een rol spelen en verantwoordelijkheid dragen.

Techniek
Over de techniek stellen we de volgende deelvragen:

Zijn het netwerk en bedrijfskritische systemen voldoende technisch beveiligd om ongeautoriseerde toegang te voorkomen?
Met een scan en eventueel een test door een specialist van PwC zal deze beveiliging getoetst worden, om zo de zwakke plekken aan te kunnen wijzen. Doel daarvan is deze zwakke plekken te verbeteren.
Is er extra aandacht voor de technische beveiliging van gevoelige informatie, zoals persoonlijke gegevens?

Het onderzoek zal specifiek aandacht schenken aan processen met gevoelige informatie, zoals persoonlijke gegevens.

2.3 Onderzoeksperiode
2013– 2017 (periode van 5 jaar) om ook de ontwikkeling hierin te kunnen aangeven.

3 Uitvoering
De rekenkamercommissie heeft een onderzoeksbureau ingehuurd voor het uitvoeren van het onderzoek. Gelet op de omvang van dit onderzoek (uit te voeren bij de vier gemeenten) zal één lid van de rekenkamercommissie het onderzoek coördineren v.w.b. het proces / voortgang. Inhoudelijk is per gemeente een lid van de rekenkamercommissie begeleider van het onderzoek.

3.1 Onderzoeksfasen
Globaal worden de volgende fasen doorlopen in het onderzoek:

1 Startbijeenkomst met de betrokken ambtenaren
2 Dossieranalyse
3 Opstellen normenkader
4 Interviews
5 Groepsgesprek met raadsleden
6 Analyse van de bevindingen
7 Opstellen concept rapportages
8 Ambtelijk hoor en wederhoor (technische reactie)
9 Opstellen definitieve rapportages, inclusief conclusies en aanbevelingen (per gemeente komt er een eigen rapportage)
10 Bestuurlijke reactie door het college van burgemeester en wethouders
11 Aanbieding van het rapport aan de raad.

3.2 Tijdpad
Het streven is het onderzoek te starten in juli. Inmiddels is er een startbijeenkomst gepland. Het onderzoek is gepland in de 2e helft van 2018. De rapportage is dan in het eerste kwartaal van 2019 gereed. Bij het opstellen van deze planning wordt uitgegaan van een flexibele medewerking van alle betrokkenen bij het onderzoek.
De belasting van het onderzoek beperkt zich tot deelname van enkele raadsleden aan een groepsinterview en van de verantwoordelijke wethouder(s) en bestuurders aan een individueel interview.
De belasting voor de gemeentelijke organisatie zal zich beperken tot het deelnemen aan interviews van de betrokken bestuurder(s) en medewerkers, het tijdig ter beschikking stellen van de complete dossiers en het reageren op de rapportversies in het ambtelijk en het bestuurlijk wederhoor.