Fractie van BOB en overige leden van de gemeenteraad

Uw brief van	Uw kenmerk	Ons kenmerk	Datum	Verzonden d.d.
1 juni 2020	S-504 (20int02421)	20UIT12993	30 juni 2020	
Onderwerp:		**Behandeld door**	**Telefoonnummer**	**Bijlage(n)**
Beantwoording schriftelijke vragen S-504 van BOB over Informatiebeveiliging DigiD en Suwinet		B. Jansen	14 0481	

Geachte fractie van BOB en overige leden van de gemeenteraad,

Op 1 juni heeft u schriftelijke vragen gesteld over de Informatiebeveiliging van DigiD en Suwinet. Met deze brief beantwoorden wij uw vragen.

Aanleiding tot uw vragen

Sinds 2015 wordt de gemeenteraad (in het kader van de verplichte horizontale verantwoording) door het College geïnformeerd over de informatiebeveiliging van DigiD en Suwinet. Dit gebeurt via informatiememo's aan de raad.

Het gaat bij DigiD en Suwinet om informatiebeveiliging die betrekking heeft op alle inwoners. Bij Suwinet gaat het om informatie die onder andere. wordt gebruikt bij kostendeling. Het belang van deze
informatiebeveiliging is onder andere ingegeven door de ervaring dat bij onvoldoende beveiliging gegevens kunnen worden ingezien die niet noodzakelijk zijn voor de door de betreffende medewerkers uit te voeren taken.

Voor het vertrouwen in de overheid is een goede informatiebeveiliging zeer belangrijk. Niet alleen omdat bij onvoldoende beveiliging, bijvoorbeeld 'de levering van gegevens via Suwinet tijdelijk kan worden opgeschort wat veel extra werk voor medewerkers en hinder voor inwoners mee zou brengen', maar ook omdat inwoners moeten weten dat dit soort privacygevoelige gegevens bij de overheid in goede handen zijn.

Sinds 2015 is bij de memo's over informatiebeveiliging DigiD en Suwinet informatie opgenomen over verbeteracties. Onze indruk was dat Overbetuwe hierbij niet bijzonder was: in heel Nederland moest op dit punt een flinke verbeterslag gemaakt worden. En in de memo uit 2015 werd gemeld dat het beveiligingsplan was geactualiseerd en dat na invoering daarvan aan alle eisen voldaan zou zijn.

Sindsdien is periodiek gerapporteerd, telkens met vermelding van eisen waar nog niet aan voldaan is en genomen verbetermaatregelen.

Sinds december 2018 wordt informatie over normen waar de gemeente niet aan voldoet, onder vertrouwelijkheid aan de gemeenteraad verstrekt. Het College motiveert dit door te stellen dat er anders risico is op misbruik door derden en dat in verband daarmee informatieveiligheid hier gaat boven openbaarheid. U schrijft dat in de openbare oplegmemo echter voor inwoners of voor generalisten als raadsleden – los van de vertrouwelijke technische details – niet duidelijk is wat de ernst is van het niet voldoen aan alle eisen. In de ogen van BOB bemoeilijkt dit het proces van horizontale verantwoording zoals de wetgever dit beoogt.

U schrijft dat in een memo van december 2019 wederom openbaar lijkt te worden aangegeven dat weliswaar niet aan alle eisen wordt voldaan, maar dat er verder geen probleem is. De gemeente is ‘in control’: er zijn voldoende verbeteracties ingezet, waarover opnieuw verantwoording zal worden afgelegd. Medio 2020 zou verantwoording worden afgelegd over de op uitzonderingen gerichte beheersmaatregelen over 2018.

Graag beantwoorden wij de volgende vragen:

1. Hoe beoordeelt het College de sinds 2016 doorlopen pdca-cycli rond informatiebeveiliging bij DigiD en Suwinet? Kunt u toelichten waarom nog steeds niet voldaan wordt aan de normen?

Informatiebeveiliging binnen de gemeente Overbetuwe haakt inderdaad aan op de PDCA-cyclus waarbij er continue aandacht is voor verbetering. Er worden dus ook continue verbeteringen in beveiligingsmaatregelen doorgevoerd.

Maar zowel de normenstelsels als de bedrijfsvoering veranderen. Concreet betekent dit dat een beveiligingsmaatregel die voldeed in 2017, niet zonder meer ook in 2020 voldoet. Enerzijds dus omdat de bedrijfsvoering, het geheel van ICT-applicaties, leveranciers, koppelingen en gegevensuitwisselingen, is veranderd. Anderzijds omdat de norm zelf is veranderd, want elk jaar wordt de lat een stukje hoger gelegd. Dit laatste is duidelijk herkenbaar in de ENSIA systematiek over de jaren. Daar waar voorheen de focus ligt op ‘opzet’ en ‘bestaan’ per norm, verschuift dit nu naar het aantonen van de ‘werking’.

Wat is ENSIA? ENSIA (Eenduidige Normatiek Single Information Audit) heeft tot doel het verantwoordingsproces over informatieveiligheid bij gemeenten verder te professionaliseren door het toezicht te bundelen en aan te sluiten op de gemeentelijke Planning & Control-cyclus. Hierdoor heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier ook beter op sturen.

Voor uw beeldvorming: voor DigiD dienen we aan 20 constant veranderende normen te voldoen, voor Suwinet 11, en voor de gehele Baseline Informatiebeveiliging Overheid zijn dit er 114. Dit grote aantal normen maakt het noodzakelijk om keuzes te maken in focusgebieden en beveiligingsmaatregelen. Ook hier geldt dat dit op basis van PDCA én risicomanagement gebeurt.

Dit leidt er toe dat we al enkele jaren niet 100% scoren op de perfecte informatieveiligheid. Dit leidt er echter wel toe dat we 100% in control zijn. Want voor elke norm die we niet halen, wordt een verbeterplan en/of extra beveiligingsmaatregel verplicht gesteld. En hierop worden we door een accountant gecontroleerd, juist ook op de uitvoering hiervan. Zo dienen we voor DigiD specifiek per september aan te tonen dat de verbeterplannen van vorig jaar zijn uitgevoerd.

Zodoende geeft de accountant, na controle, dan ook elk jaar aan dat we ‘in control’ zijn. De raad ontvangt dit accountantsverslag.

2. Is er naar de beoordeling van het College een probleem in relatie tot onze inwoners als onbevoegden inzage kunnen krijgen in zeer privacy-gevoelige gegevens of is er alleen een probleem als dat leidt tot handhavend optreden van de Rijksoverheid?

Als onbevoegden inzage kunnen krijgen in privacy gevoelige gegevens is dat altijd een probleem, los van het feit dat instanties vanuit de Rijksoverheid (bijvoorbeeld de Autoriteit Persoonsgegevens) dan handhavend kunnen optreden. Gemeente Overbetuwe is namelijk verantwoordelijk voor de verwerking en dus bescherming van de vele gevoelige gegevens van haar inwoners en bedrijven. Deze gegevens worden óf rechtstreeks beheerd, óf zijn benaderbaar via gemeentelijke systemen. Bij toegang door onbevoegden kan zowel de beschikbaarheid, integriteit als vertrouwelijkheid van deze gegevens niet meer gegarandeerd worden. Dat kan grote impact hebben op de dienstverlening, maar ook het imago van de gemeente. Kortom het is in het belang van de gemeente om adequaat beveiligd te zijn en het toetsen vanuit het Rijk helpt ons daarbij.

3. Heeft het College via zaken als autorisatie en logging voldoende inzicht in de mate waarin door medewerkers mogelijk onnodig privacy-gevoelige gegevens zijn ingezien? Zo nee, waarom niet? Zo ja, is het College bekend of er gevallen zijn waarin dit is gebeurd en als er gevallen zijn waarin dit is gebeurd, hoe is daar dan in opgetreden en welke sancties zijn daarbij toegepast? Zijn er in dit verband relevante meldingen geweest bij onafhankelijke derden, zoals de Autoriteit Persoonsgegevens?

Op Suwinet en DigiD wordt er gelogd en er vinden periodieke controles plaats aan de hand van deze logging. Een functioneel beheerder controleert periodiek of het gebruik van de applicatie nog rechtmatig is voor een bepaalde medewerker. De veiligheidsfunctionaris controleert dit óók (steekproefsgewijs). Hiermee is een dubbel controle mechanisme ingericht. Specifiek op deze onderwerpen wordt ook door de accountant gecontroleerd.

Er zijn situaties voorgekomen waarbij een medewerker onterecht toegang heeft gekregen tot vertrouwelijke gegevens. In deze zeldzame gevallen werd er door een administratieve (menselijke) fout een medewerker in een verkeerde rol geplaatst (bijvoorbeeld bij indiensttreding), en dus onterecht geautoriseerd. In al deze gevallen is er snel opgetreden door de verantwoordelijke lijnmanager en is dit hersteld. In het kader van voorgaande is het niet nodig geweest de Autoriteit Persoonsgegevens in te lichten. Daar waar toegang onterecht mogelijk was, wil dat niet zeggen dat hier ook gebruik is gemaakt. Het betrof in deze gevallen collega's werkzaam bij de gemeente die gehouden zijn aan hun integriteitsbelofte of -eed waarmee ze gehouden zijn om geen informatie met derden te delen.

De Gemeente Overbetuwe houdt ook een datelekregister bij, waarin alle privacy gerelateerde incidenten (intern en extern) kunnen worden geregistreerd.

4. Wanneer kan de voor medio 2020 aangekondigde verantwoording over de op uitzonderingen gerichte beheersmaatregelen over 2018 bij Suwinet en DigiD worden verwacht?

De noodzakelijke verbeteringen en beheersmaatregelen over 2018 zijn inmiddels doorgevoerd. Deze waren van kracht in 2019. Over dit jaar heeft het college opnieuw verantwoording afgelegd. Hierover is de raad op 31 maart 2020 geïnformeerd (ENSIA).

Echter, over 2019 zijn nieuwe op uitzonderingen gerichte beheersmaatregelen noodzakelijk. Op moment van schrijven zijn de verantwoordelijke medewerkers druk bezig om deze verbeteringen

door te voeren. Uiterlijk in september 2020 dienen we de verbeteringen voor te leggen aan Logius, de uitvoerende instantie vanuit het ministerie van BZK. Met andere woorden, de verbeteringen (noodzakelijk over 2019) moeten in september 2020 zijn doorgevoerd. Ook hier geldt dat een accountant de verbeteringen dan moet verifiëren. De raad kan daarna een terugkoppeling verwachten. Deze zal plaatsvinden over het hele jaar 2020 in het kader van ENSIA en volgt begin 2021.

Daarnaast zal de raad ook middels een informatiebijeenkomst (onderwerp ‘informatieveiligheid’) geïnformeerd worden. Dit zal nog dit jaar gebeuren (Q3).

5. Wanneer kan de raad over 2019 een jaarrapportage / jaarverslag van de functionaris gegevensbescherming (FG) ten behoeve van de gemeenteraad tegemoet zien op basis van het recent door de VNG ontwikkelde model?

De raad kan deze rapportage uiterlijk in de tweede helft van augustus verwachten.

Hoogachtend,

burgemeester en wethouders,
de gemeentesecretaris, de burgemeester,

mr. M.F.H. Knaapen R.P. Hoytink-Roubos