

Reactie op het verslag van bevindingen EY

Niet alle onderwerpen die in het verslag van bevindingen aan de orde worden gesteld behoeven een reactie. Hieronder zijn daar waar dit relevant is geacht de reacties weergegeven.

Noodzakelijke verbeteractie en/of advies	Reactie
1. <u>Uw begrotingsbeheer is voor verbetering vatbaar</u> Uw raad is actief geïnformeerd over (financiële) ontwikkelingen binnen uw gemeente. Wel merken wij hierbij op dat enkele –voorzien –incidentele baten en lasten niet tijdig zijn verwerkt in een u aangeboden begrotingswijziging. Hierbij denkend aan bovenstaande overschrijding van €3,6 miljoen op het vastgoed Stationsplein en onderschrijding van €4,5 miljoen binnen het sociaal domein. Dit als gevolg van de eind december 2016 door uw raad vastgestelde Visie op het Stationsgebied en onvoldoende tussentijds zicht op de (verwachte) bestedingen binnen het sociaal domein. Daarnaast is sprake van een overschrijding van €3,1 miljoen binnen het saldo kostenplaatsen en een onderschrijding van €1,2 miljoen voor de vrijval van de gepassiveerde ISV middelen. Qua snelheid van begrotingsanalyse en –verwerking zou het proces rond begrotingsbeheer daarmee in informatiewaarde kunnen toenemen. Ons advies is uw raad eerder te informeren over dergelijke over- en onderschrijdingen middels een raadsinformatiebrief of voorstel tot begrotingswijziging.	Volgens ons huidige en nieuwe financiële beleid worden begrotingsafwijkingen die gedurende het jaar al bekend waren tijdens het jaar zelf nog aan de raad voorgelegd. Afwijkingen waarbij dat niet mogelijk was worden in de jaarrekening goed toegelicht door te verwijzen naar raadsbesluiten of informatieverstrekking aan de raad. Zo maakt het college duidelijk waarom het vindt dat de afwijkingen passen binnen het door de raad vastgestelde beleid. In het geval van de overschotten binnen het sociaal domein zijn wij in belangrijke mate afhankelijk van de rapportages vanuit de Regio. Het college neemt de aanbeveling ter harte en zal gedurende het jaar de raad actiever en vooral vroegtijdiger informeren middels de onderhanden zijnde dashboards. In het specifieke geval van de afwaardering voormalig Gak gebouw zijn wij als college van mening dat wij de raad vroegtijdig geïnformeerd hebben over de financiële consequenties. Met betrekking tot de ISV middelen is de raad vroegtijdig geïnformeerd en hebben wij gedurende het jaar de begroting ook aangepast met 3,4 mio. Ten tijde van de jaarrekeningcontrole is gebleken dat de resterende 1,2 mio volledig kon vrijvallen. Het college stelt in het algemeen dat in ons nieuwe financiële beleid de raad actief en vooral sneller wordt geïnformeerd door middel van RIB's dan wel Raadsvoorstellen met als aanvulling 2x per jaar een tussenrapportage waarin wij de begroting ook daadwerkelijk zullen aanpassen voor de afgesproken omvang van afwijkingen.
2. <u>Paragraaf weerstandsvermogen</u> Wij merken op dat de paragraaf weerstandsvermogen in informatiewaarde kan toenemen, door hierin expliciet stil te staan bij de ontwikkeling bij de ingeschatte risico's en de weerstandscapaciteit ten opzichte van de voorgaande jaarrekening. De paragraaf biedt hier momenteel beperkte mogelijkheden toe.	Het college neemt deze aanbeveling over. In het verleden hebben wij niet op deze wijze naar de risicoparagraaf gekeken. Wij hebben de focus gelegd op een duidelijke beschrijving van de risico's en de wijze waarop het weerstandsvermogen berekend wordt. Daarnaast streeft het college ernaar de omvang van de begroting en jaarstukken te reduceren. Bij het opstellen van de volgende paragraaf, zullen wij beoordelen hoe wij de informatiewaarde daadwerkelijk kunnen verbeteren en de benodigde uitbreiding in de paragraaf opnemen.
3. <u>Inkoop en aanbesteding</u> De controle op de naleving van de Europese aanbestedingsregels is nog onderhanden. De verbijzonderde interne controle heeft de interne controle op de naleving van de Europese aanbestedingsregels verricht. Wij merken op dat uit deze interne controle bevindingen volgen, die een impact kunnen hebben op de strekking van ons oordeel bij de rechtmatigheid van de jaarrekening. Deze bevindingen zien toe op €0,8 miljoen aan onrechtmatig aanbestede uitgaven voor 2016, waarbij de Europese aanbestedingsregels ten onrechte niet zijn gevolgd. Bekeken over de gehele contractperiode betreft dit een geraamde onrechtmatigheid van €1,5 miljoen. De verbijzonderde interne controle merkt op dat de geconstateerde onrechtmatigheden volgen uit een bewuste afweging van gemeente Hilversum tot het niet in gang zetten van een Europese aanbesteding. Als gevolg hiervan heeft de afdeling foutevaluatie verricht naar	Het college stelt dat in twee van de 3 zelf geconstateerde inkooponrechtmatigheid bewust gekozen is om af te wijken van geldende regelgeving. De bij de verbijzonderde controle naar voren gekomen onrechtmatigheden, zijn bekend bij concern inkoop en reeds opgepakt. Hierbij moet in het geval van de microsoft licenties rekening gehouden worden met lopende oude contracten, die in het verleden zijn afgesloten en waar we nu als organisatie de pijn van ondervinden. Concerninkoop heeft in het algemeen middels een spendanalyse van 2015 de risicovolle inkooptrajecten in kaart gebracht. Naar aanleiding van deze analyse en de eerdere bevindingen van de accountant en diepgaande interne controle zijn er verschillende Europese aanbestedingen uitgevoerd. Alle inkooptrajecten op de inkoopagenda worden volgens planning opgepakt en rechtmatig en doelmatig aanbesteed, zodat de achterstand dan wel onrechtmatigheden van het

soortgelijke gevallen, hetgeen leidt tot de volgende –interne – conclusies. De bevindingen betreffen de onrechtmatige aanbesteding van: ► Groot onderhoud openbare ruimte Tomin €0,4 miljoen; ► Onderhoud lichtmasten Dynnig€0,2 miljoen; ► Licenties Fujitsu €0,2 miljoen.	verleden wordt weggewerkt en het foutpercentage steeds kleiner wordt. Hierdoor wordt het risico op onrechtmatige uitgaven geminimaliseerd en zo wordt het aandeel rechtmatige contracten steeds groter. ► Groot onderhoud openbare ruimte Tomin € 0,4 miljoen → betreft een bewuste keuze door het college vanuit zwaarwegende redenen in het werkvoorzieningschap regionaal en hierover is de raad al geïnformeerd met inbegrip van de gevolgen voor de jaarrekening 2016 en 2017. ► Onderhoud lichtmasten Dynnig € 0,2 miljoen → betreft een bewuste keuze door het college in afwachting van de regionale aanbesteding samen met gemeente Gooise Meren. ► Licenties Fujitsu € 0,2 miljoen → betreft oud contract De aanbesteding destijds in 2014 is niet via Europese richtlijnen gegaan. Inmiddels heeft er wel een Europese aanbesteding plaatsgevonden, maar door de looptijd van het oude contract vallen de Microsoft licenties pas vanaf 2018 onder het nieuwe contract standaard software. Met de aanbesteding van dit contract is de rechtmatigheid in de toekomst geborgd.
4. <u>Activaregistratie</u> In 2016 heeft een grondige inventarisatie plaatsgevonden van het materiële vaste activa bestand, wat heeft geleid tot een financieel nadeel van €1,1 miljoen. Dit nadeel bestaat uit: ► Het desinvesteren van activa (voormalige schoolgebouwen) die niet meer in het bezit zijn van de gemeente voor €0,9 miljoen; ► Het desinvesteren van activa met een omvang kleiner dan €10.000, hetgeen onder de nota “Investerings, waarderingen en activering” niet voor activering in aanmerking komt, voor €0,2 miljoen; ► Het desinvesteren van geactiveerde verkoopopbrengsten van onderwijsgronden van €1,3 miljoen. De hiermee gerealiseerde opbrengst is budgetneutraal gestort in de bestemmingsreserve Onderwijsgebouwen. De doorgevoerde aanpassing in de gepresenteerde en gewaardeerde materiële vaste activa vormt fouterstel. Gemeente Hilversum heeft de fout geanalyseerd als niet-fundamentele fout en ten laste van het resultaat 2016 verwerkt. Een fout is fundamenteel als deze voor het aan uw raad geboden inzicht onontbeerlijk is. Wij verenigen ons met de analyse van uw gemeente dat de fout niet-fundamenteel is. De aanwezige fout geeft aanleiding de interne procedures en richtlijnen voor het volgen van de nota “Investerings, waarderingen en activering” aan te scherpen. De interne beheersing heeft op dit vlak onvoldoende gefunctioneerd om de fout te ontdekken. Wij adviseren u de bestaande procedures hiertoe te herijken. Hierbij kan worden gedacht aan het betrekken van de controle van de materiële vaste activa mutaties en –bestand in de verbijzonderde interne controle.	Het college neemt deze aanbeveling over. Waar in het verleden de zogenaamde ‘checks & balances’ op dit gebied onvoldoende hebben gewerkt, kunnen we stellen dat de IC in 2016 wel heeft gewerkt, want zo is naast de grondige inventarisatie van het materiële activa bestand mede het financiële nadeel bepaald. In 2016 is door onze eigen interne controle de fout geconstateerd en hersteld. Het college ziet erop toe dat dit nu ook voldoende geborgd gaat worden in het nieuwe financiële beleid en dan met name in de nadere uitvoeringsregels.
5. <u>Benuttingmiddelen Investeringsbudget Stedelijke Vernieuwing (ISV)</u> Gemeente Hilversum heeft uit het Ontwikkelingsprogramma Stedelijke Vernieuwing 2010-2014 en het Investeringsbudget Stedelijke Vernieuwing 2005-2009 in totaal €11,3 miljoen ontvangen van provincie Noord-Holland. Door onvolledige uitvoering van de projecten is het onbenutte deel van de	Aanbeveling is inmiddels verwerkt in de jaarstukken. Zie bevinding.

subsidie van €5,4 miljoen ultimo 2015 als overlopende passiefpost verantwoord. Provincie Noord-Holland heeft de subsidies in 2016 definitief vastgesteld. Vrijval van de gevormde middelen dient daardoor plaats te vinden als gerealiseerde bate. De vrijval van de resterende overlopende passiefpost van €1,2 miljoen merken wij als controleverschil aan en is in de aan u voorliggende jaarstukken op een juiste wijze gecorrigeerd.	
6. Overdrachtbeheer en onderhoud begraafplaatsen Wij adviseren u de governance-organisatie op de door de stichting beheerder middelen adequaat in te richten. Dit om de juiste en rechtmatige besteding van de aan de stichting vertrouwde middelen te garanderen. Hierbij kan gedacht worden aan het inregelen van de benodigde bestuurlijke governance middels directe betrokkenheid van gemeente Hilversum in een bestuurs-of toezichtsfunctie. Uw wethouder neemt namens de gemeente deel in het bestuur van de stichting. Daarnaast is aan te raden verantwoordings-informatie te verlangen van de stichting over de inzet van de bestede middelen. Hierbij is het aan te raden deze informatie door een externe accountant te laten controleren bij een door uw raad opgesteld protocol met door u gestelde eisen aan de financiële verantwoording. Wij hebben begrepen dat een externe accountant bij de stichting is betrokken. Wij adviseren u de voorgaande elementen in overweging te nemen bij de formulering van de hem toegekende opdracht.	Het college neemt deze aanbeveling over en zijn van mening, dat de aanbeveling al ter hand is genomen: • M.b.t. de governance merken wij op dat de wethouder voorzitter is van de Raad van Toezicht van de stichting. • Hoe de stichting zijn verantwoordingsinformatie, waaronder de begroting en de jaarrekening, periodiek met de gemeente moet delen is nauwkeurig geregeld in de stichtingsstatuten. • Het is het stichtingsbestuur, dat opdracht verleent aan de accountant, die de stichting controleert. Of de stichtingsaccountant zich daarbij op een gemeentelijk protocol zou moeten baseren zullen wij in 2017 overwegen. Het college is zich er terdege van bewust dat regie op verbonden partijen essentieel is en verder vorm moet gaan krijgen.
7. Corruptie-en omkopingsrisico's Uw gemeente maakt onderdeel uit van de overheidssector waarin corruptie vaker dan bij andere sectoren voorkomt. Dit komt onder andere omdat veel transacties met een relatief grote omvang zijn, de transparantie over marktprijzen niet in alle gevallen voldoende is om te beoordelen en frequent zaken gedaan wordt met andere corruptiegevoelige sectoren (vastgoed, constructie, infrastructuur et cetera). Hierdoor hebben wij dit als aandachtspunt in onze controle meegenomen. Corruptie is een wereldwijd probleem waar het ook uw verantwoordelijkheid is om corruptie binnen uw gemeente te voorkomen. Onze beroepsregels zijn in de praktijkhandreiking "Corruptie, een relevant onderwerp in het kader van (controle) werkzaamheden van de accountant" verder aangescherpt, hetgeen tot aanvullende werkzaamheden heeft geleid. Wij constateren dat u geen overkoepelende risicoanalyse / anti-corruptiebeleid hebt opgesteld. In plaats hiervan is binnen uw organisatie van verschillende maatregelen als onderdeel van de operationele processen waaronder: ► Indiensttreding van (tijdelijk) personeel: antecedentenonderzoek, ambtseed etc.; ► Personeelsbeleid omtrent het aannemen / verstrekken van giften; ► Inkopen en factuurverwerking: registratie door administratie, goedkeuring door budgethouder aangevuld met een gegevensgerichte toets door de verbijzonderde interne controle op de prestatielevering; ► Aanbestedingen: operationalisering intern inkoopbeleid in de vorm functiescheiding / betrokkenheid meerdere functionarissen bij het traject omtrent contractvorming met leveranciers; ► Omgevingsvergunningen: betrokkenheid van meerdere functionarissen bij het verstrekken van vergunningen evenals handhaving door de afdeling handhaving;	Het college neemt de aanbeveling grotendeels over door dit in het huidige integriteitsbeleid specifiek aandacht te geven. In het najaar wordt er een onderzoek gedaan of en hoe er verder vorm aan kan worden gegeven. Vooralsnog betekent dit niet automatisch een overkoepelend anti corruptiebeleid. We herkennen de bevindingen van EY en zijn verheugd dat de 'checks & balances' in de specifieke operationele processen gewerkt hebben. Het college is voornemens bij het onderzoek de handreiking van de VNG te volgen. Integriteit is als een van de zeven leidende beginselen opgenomen in de Nederlandse code voor Goed Bestuur. Openheid en integriteit worden daarbij in samenhang gezien met de andere voorwaarden voor goed bestuur dat zich kenmerkt door behoorlijk bestuur (met kernwaarden als integriteit, gelijkheid en rechtmatigheid), responsief bestuur (legitimiteit, openheid, participatie en verantwoording) en resultaatgericht bestuur (effectiviteit en efficiency). De taken, bevoegdheden en verantwoordelijkheden van het college zijn wettelijk geregeld. Het is van groot belang dat het college voor de juiste checks en balances zorgt als zij haar bevoegdheid uitoefent of laat uitvoeren door de interne dan wel verbonden organisaties. Daarbij wordt meer en meer actief rekening gehouden met eventuele integriteitsrisico's en is het integriteitsbewustzijn door de hele organisatie gestimuleerd en geborgd.

► Verkopen van vaste activa: verkoopprijs is gebaseerd op externe taxatierapporten / intern prijsbeleid. In geval van afwijkingen dienen deze, afhankelijk van aard / omvang te worden goedgekeurd door college / raad. Gedurende onze controle hebben wij gegevensgericht, op basis van een deelwaarneming, transacties gecontroleerd en hebben hierbij de betreffende maatregelen terug zien komen. Op basis van deze werkzaamheden hebben wij geen bevindingen geconstateerd. Wel adviseren wij u een overkoepelend anti-corruptiebeleid op te stellen en te implementeren, waar nodig aangevuld met trainingen. In het verlengde hiervan adviseren wij u ook peridook te toetsen of de maatregelen als opgenomen in dit beleid zichtbaar worden nageleefd.	
8. <u>Meldplicht datalekken</u> Bij overtreding van de meldplicht datalekken kan de Autoriteit Persoonsgegevens een boete uitdelen. Deze boete kan oplopen tot maximaal €820.000 voor overtreding van de meldplicht datalekken uit de Wet bescherming persoonsgegevens. Voor overtreding van de meldplicht uit de Telecommunicatiewet kan de boete oplopen tot maximaal €900.000. Wij adviseren u om na te gaan in hoeverre de gemeente Hilversum bovenstaande in beeld heeft en passende maatregelen heeft getroffen.	Het college neemt deze aanbeveling over. In 2016 zijn er 34 beveiligingsincidenten gemeld 1 datalek hiervan is in het jaar 2016 gemeld bij de Autoriteit Persoonsgegevens. Het ging hierbij om een structurele lek waarbij de papierencontainers die buiten staan om opgehaald te worden niet op slot konden en er gevoelige persoonsgegevens in zijn gevonden. Dit is gemeld aan de Autoriteit Persoonsgegevens en de containers gaan nu altijd op slot en de medewerkers zijn geïnstrueerd om vertrouwelijke informatie te versnipperen. In 2017 zijn er nog 6 meldingen bijgekomen waarbij er 2 zijn gemeld bij de Autoriteit Persoonsgegevens. 1 melding had te maken met het feit dat bij belastingen BSN nummers zichtbaar zijn op het adresvenster. Er is voor gekozen de BSN geheel van het formulier af te halen. De tweede melding betrof het vermeend (door de pers gesuggereerd) verkeerd gebruik van het twitteraccount van de burgemeester. Achteraf bleek dat dit niet het geval was, en dat er geen sprake was van een datalek. Incidenten worden altijd opgepakt, afhankelijk van de urgentie vind afhandeling direct plaats of wordt gekeken of het treffen van maatregelen kan worden opgenomen in de actielijst. Meeste incidenten hebben weinig invloed gehad op de persoonlijke levenssfeer van de burger. Dit betrof incidenten zoals het verkeerd versturen van een paspoort naar diverse medewerkers, het niet afsluiten van een bewerkersovereenkomst of het delen van inloggegevens met anderen. Wel zijn hier maatregelen op getroffen. Voor deze incidenten is er voor gekozen dit niet te melden bij de Autoriteit Persoonsgegevens. In maart 2017 zijn we gestart met het actualiseren van de informatieveiligheidsanalyse, dit zorgt voor een actueel beeld van de voortgang van de implementatie van de BIG. Vervolgens gaan we het Plan van Aanpak Informatieveiligheid in het najaar actualiseren.
9. <u>► Privacy van gegevens binnen het sociaal domein.</u> Binnen het sociaal domein vindt registratie van persoonsgegevens plaats binnen de twee kernapplicaties GWS4all (op gemeenteniveau) en het DLP van de Regio Gooi- en Vechtstreek. Wij merken dat afscherming van privacygegevens in de basis goed plaatsvindt door de getroffen functiescheidingen binnen de applicaties. Echter, een overkoepelend beeld van de verschillende momenten wanneer en waarop registratie en uitwisseling van –potentieel gevoelige –gegevens plaatsvindt, ontbreekt momenteel binnen uw gemeente. Hierbij denken wij aan uitwisseling van gegevens via USB-gegevensdragers, e-mail of lokale opslagschijven. De controle op een adequate afscherming van privacygegevens via deze gegevensdragers vindt veelal via een minder gereguleerd omgeving plaats.	Het college neemt deze aanbeveling over. Om de privacy binnen het sociaal domein goed te waarborgen, heeft de VNG een raamwerk ontwikkeld. Dit zijn vijf gebieden, die met elkaar samenhangen: Governance, beleid, werkprocessen en triage, bewustwording en training, beheer en opslag. Dit zijn de randvoorwaarden om de privacy op orde te brengen binnen het sociaal domein. • <u>Governance:</u> Zorg voor eigenaarschap voor het onderwerp privacy het onderwerp moet blijven leven.

Wij merken dan ook op dat uw gemeente risico's loopt ten aanzien van de opslag en het beheer van privacygevoelige informatie. Wij adviseren u hieromtrent een alomvattend privacy beleid te implementeren, waarbij begonnen wordt bij de vraag welke privacygevoelige informatie uw gemeente binnen het sociaal domein registreert. Dit mede ingegeven door de nieuwe Algemene Verordening Gegevensbescherming (AGV) met ingangsdatum 25 mei 2018. Vervolgens dient via een risico-analyse inzichtelijk te worden gemaakt op welke plekken in uw organisatie deze informatie wordt opgeslagen en waar zwakke schakels zich bevinden betreffende beveiliging. Rond beheer van privacygevoelige informatie is het daarnaast vooral belangrijk de gebruikers binnen uw organisatie actief te informeren over het geldende privacy beleid en de "do's and don'ts" op dit vlak. Vindt uw gemeente het bijvoorbeeld acceptabel dat privacygevoelige informatie via USB-stick of e-mail wordt overgedragen? Het is hierbij van belang aan de hand van deze wensenlijst het privacy beleid verder op te tuigen, waarbij voorrang wordt gegeven aan de elementen in het privacy beleid die u als risicovoller beschouwt.	De business controller kan de kwaliteit op het gebied van privacy controleren en hierover rapporteren. • <u>Beleid:</u> Leg de afspraken omtrent gegevensuitwisseling met samenwerkingspartners vast in een privacy convenant. Met de huisarts is er al een concept convenant. Met de overige samenwerkingspartners dienen afspraken nog te worden vastgelegd, • <u>Werkprocessen en triage:</u> Bepaal d.m.v. triage wanneer beslissingen over gegevensuitwisseling worden genomen. Leg de stappen en afwegingen vast in de werkprocessen. • Maak concreet voor welke wettelijke taken welke persoonsgegevens noodzakelijk zijn. Vraag alleen de persoonsgegevens uit die noodzakelijk zijn voor het uitvoeren van de taak. (BSN altijd nodig?). • Vraag toestemming aan de burger wanneer deze vrij, specifiek en geïnformeerd gegeven kan worden. Wanneer verwerk je bijvoorbeeld gegevens zonder toestemming?: Leg dit vast in een instructie. • Informeer de burger over welke gegevens worden verwerkt en waarom. Leg uit wat de rechten zijn van de burger. (Recht op correctie, inzage en vernietiging). • <u>Bewustwording en training:</u> Organiseer bewustwording voor de professionals. Het LBVD (Awareness bureau) kan door middel van workshops professionals handvatten geven hoe om te gaan met privacy. (offerte is hier al voor opgevraagd). Daarnaast kan het onderwerp privacy aan bod komen tijdens casuïstiek overleggen. • <u>Beheer en opslag:</u> Bepaal hoe persoonsgegevens geregistreerd, gedeeld en openbaar gemaakt worden. Wat wordt opgeslagen en waar? Hoe lang blijven gegevens bewaard? Wie mag de gegevens inzien en wie controleert dat? Waar worden de medische gegevens opgeslagen? Het belang van het onderwerp privacy is al onder de aandacht gebracht. De bovenstaande aanbevelingen van de VNG zullen verder worden uitgewerkt en zijn gekoppeld aan vervolgacties.
---	--

Algemene opmerking van EY

Ten opzichte van voorgaand jaar hebben wij onze controleaanpak gewijzigd, waarbij wij in meerdere mate gegevensgerichte controlewerkzaamheden verrichten (steekproeven, deelwaarnemingen en detailcontroles) in plaats van systeemgerichte controlewerkzaamheden (gericht op het testen van de werking van interne beheersing). Deze wijziging is het gevolg van een algehele ontwikkeling binnen het accountantslandschap, waarbij de nadruk steeds meer komt te liggen op het door de accountant zelfstandig verrichten van gegevensgerichte controlewerkzaamheden teneinde tot zijn oordeel te komen.

De oorzaak hiervan ligt voor een deel in het verscherpte toezicht vanuit de Autoriteit Financiële Markten (AFM) op de accountants waardoor omvang en intensiteit van de werkzaamheden die de accountant bij ons moet verrichten is toegenomen. Zowel de accountant als wij moeten wennen aan en anticiperen op deze aanscherpingen.