Deloitte.

Managementletter 2018

Regionale Belasting Groep

19 maart 2019

Deloitte.

Deloitte Accountants B.V.
Wilhelminakade 1
3072 AP Rotterdam
Postbus 2031
3000 CA Rotterdam
Nederland

Tel: 088 288 2888
Fax: 088 288 9830
www.deloitte.nl

Aan het dagelijks bestuur van de
Regionale Belasting Groep (RBG)
T.a.v. de heer H. Sigmond (directeur)
Postbus 923
3100 AX SCHIEDAM

Datum
19 maart 2019

Behandeld door
H. de Winter
088 288 0417

Ons kenmerk
2019.063088/LR

Geachte leden van het dagelijks bestuur,

Wij hebben conform onze opdrachtbevestiging d.d. 29 november 2018, als onderdeel van de controle van de jaarrekening en de jaarverantwoordingen 2018, de interim-controle voor de Regionale Belasting Groep (hierna: de RBG) uitgevoerd. Deze controle is primair gericht op de analyse en evaluatie van de interne-beheersings-omgeving en de daarin opgenomen maatregelen van interne controle. In onze managementletter zijn onze bevindingen en aanbevelingen ter zake opgenomen. Tevens heeft deze controle als doelstelling om de aandachtspunten voor de jaarrekening 2018 te signaleren en onder uw aandacht te brengen.

Volledigheidshalve merken wij op dat onze analyse en evaluatie is uitgevoerd in het kader van de door u verstrekte opdracht tot controle van de jaarrekening. De geselecteerde werkzaamheden zijn afhankelijk van de door de accountant toegepaste oordeelsvorming, met inbegrip van het inschatten van de risico's dat de jaarrekening een afwijking van materieel belang bevat als gevolg van fraude of fouten. Bij het maken van deze risico-inschattingen neemt de accountant de interne beheersing in aanmerking die relevant is voor het opmaken en het getrouwe beeld van de jaarrekening en voor de rechtmatige totstandkoming van de baten, lasten en balansmutaties, gericht op het opzetten van controlewerkzaamheden die passend zijn in de omstandigheden.

De risico-inschattingen hebben niet tot doel een oordeel tot uitdrukking te brengen over de effectiviteit van de interne beheersing, de opzet, het bestaan, de effectiviteit en de efficiency van de interne beheersing als geheel en bestrijkt daarom niet noodzakelijkerwijs alle in de interne organisatie vervatte tekortkomingen.

De bevindingen en aanbevelingen kunnen worden gelezen als constructieve aanwijzingen voor het dagelijks bestuur als onderdeel van het continue proces van het veranderen en verbeteren van de beheersing van de bedrijfsvoering en de kwaliteit van de jaarrekening.

Graag lichten wij deze rapportage en onze bevindingen en aanbevelingen nader aan u toe.

Hoogachtend,

Deloitte Accountants B.V.

drs. R.M.J. van Vugt RA

Inhoudsopgave

Bestuurlijke samenvatting

Onze hoofdboodschap aan de RBG

Adviezen naar aanleiding van de bevindingen

Als onderdeel van de interim-controle 2018 hebben wij de administratieve organisatie en interne beheersing (AO/IB) van uw processen beoordeeld. Naar aanleiding van onze bevindingen zien wij geen verhoogde risico's voor onze controle.

Vooraf merken wij op dat de oplevering van de gevraagde stukken voor aanvang van onze controle tijdig en juist heeft plaatsgevonden.

Een belangrijk aandachtspunt bij de RBG betreft het proces van de memoriaalboekingen. Uit onze controle is gebleken dat de memoriaalboekingen niet vooraf worden geaccordeerd en dat deze nog onvoldoende zijn onderbouwd. Het ontbreekt hierbij aan een verwijzing naar de aanwezige digitale onderbouwing. Dit verhoogt het risico op foutieve boekingen in uw administratie, evenals het risico dat de tussentijdse informatievoorziening onjuist is.

Opvolging eerdere aanbevelingen

De managementletter 2017 bevatte diverse aanbevelingen. Tijdens de interim-controle is de follow-up van deze adviezen inzichtelijk gemaakt. In de tabel hiernaast is dit weergegeven. Hieruit blijkt dat de meeste aanbevelingen zijn opgevolgd.
De belangrijkste bevinding die naar ons inzicht op korte termijn dient te worden opgevolgd, is de volgende:

Het uitvoeren van een voldoende onderbouwde EU-aanbestedingsscan, om op deze wijze vast te stellen dat u hebt voldaan aan de Europese richtlijnen voor aanbesteden.

Follow-up aanbevelingen 2017	
Niet opgelost	1
Gedeeltelijk opgelost	2
Opgelost	1
Nog te beoordelen	0
Totaal	**4**

Bevindingen en adviezen

Onze bevindingen van de interim-controle 2018 samengevat

1. Factuurverwerking en betalingen – Onvoldoende functiescheiding in Exact Globe	• Functiescheiding bij wijziging crediteurenstamgegevens ontbreekt. Daarnaast kunnen boekingen achteraf ook worden gewijzigd, zonder dat dit geautoriseerd hoeft te worden.
2. Factuurverwerking – Onjuiste verantwoording van facturen	• Facturen die betrekking hebben op meerdere jaren worden slechts in één boekjaar geboekt. Hierdoor is de presentatie van de kosten onjuist. Daarnaast is vastgesteld dat er kosten op een onjuist grootboek worden verantwoord.
3. Inkoop en aanbestedingen – Niet structureel hanteren van inkoopplannen	• Niet voor elke inkoopopdracht wordt een inkoopplan opgesteld. Dit is wel noodzakelijk op basis van uw beleid.
4. Memorialen – Geen periodieke zichtbare controle en ontbreken van een deugdelijke onderbouwing	• De memoriaalboekingen over 2018 waren op het moment van onze controle niet gecontroleerd voorafgaand aan de inboeking. Daarnaast waren deze ook onvoldoende onderbouwd.
5. Bevindingen interne controle op gebruik uitsluiting en vrijstellingscode	• Naar aanleiding van de uitgevoerde interne controle zijn er bevindingen vastgesteld die afgewikkeld moeten worden.
6. IT-audit	• Stand van zaken is vermeld.

Bevindingen en adviezen

Toelichting bevinding 1. Factuurverwerking en betalingen – onvoldoende functiescheiding in Exact Globe

Bevinding	Wij hebben vastgesteld dat functionarissen die invoerrechten hebben in Exact Globe de crediteurenstamgegevens kunnen wijzigen. In Exact Globe is geen functiescheiding aangebracht tussen mutatie crediteurenstamgegevens en autorisatie crediteurenstamgegevens. Dit betekent dat de personen die de betaaladvieslijsten uitdraaien en controleren de crediteurenstamgegevens kunnen wijzigen, wat het risico op onrechtmatige betalingen verhoogt. Daarnaast hebben wij vastgesteld dat er achteraf wijzigingen kunnen worden doorgevoerd, nadat facturen de volledige goedkeuringsflow hebben doorlopen. Hierop vindt geen controle meer plaats. Hierdoor kunnen er wijzigingen worden aangebracht zonder dat hiervoor autorisatie plaatsvindt. Dit kan dan ook leiden tot het verantwoorden van kosten op onjuiste grootboekrekeningen.
Advies	Op basis van onze bevindingen adviseren wij u: a. Functiescheiding in Exact Globe aan te brengen tussen de invoerende en de autoriserende functionaris. b. De betaaladvieslijst te laten controleren door een medewerker met beperkte rechten in Exact (geen rechten met betrekking tot betalingsverkeer en mutaties crediteurenstamgegevens). Dit waarborgt dat er geen mutaties kunnen worden doorgevoerd zonder dat hier een controle op plaatsvindt. c. Het werken met periodeafsluitingen in te voeren. d. De functionaliteit om achteraf boekingen te kunnen muteren slechts bij een beperkt aantal medewerkers ingeschakeld te laten. Achteraf kan dan worden vastgesteld welke mutaties nog zijn doorgevoerd. Deze kunnen dan alsnog worden geautoriseerd. Op deze wijze kunt u de juistheid van uw administratie waarborgen. e. Op basis van de aanwezige logging in Exact periodiek een interne controle te laten uitvoeren op de juistheid van de doorgevoerde wijzigingen in de crediteurenstamgegevens.
Aanvullende werkzaamheden	Naar aanleiding van onze bevindingen moeten er aanvullende werkzaamheden worden verricht. Deze hebben betrekking op: 1. Juistheid mutaties crediteurenstamgegevens 2. Juistheid en rechtmatigheid betalingen 3. Juistheid mutaties a.d.h.v. ontvangen facturen Deze aanvullende werkzaamheden moeten afgerond zijn voor de start van de jaarrekeningcontrole.

Bevindingen en adviezen

Toelichting bevinding 2. Factuurverwerking – onjuiste verantwoording van facturen

Bevinding	Op basis van een steekproef hebben wij een controle uitgevoerd op de juiste verantwoording van de inkoopfacturen binnen uw administratie. Hierbij hebben wij vastgesteld dat niet alle facturen op een juiste wijze zijn verantwoord in de administratie. Eén fout heeft betrekking op het niet in het juiste jaar verantwoorden van kosten. Bij 1 van de 24 gecontroleerde facturen hebben wij vastgesteld dat de kosten betrekking hebben op meerdere jaren, maar geboekt zijn ten laste van 2018. Dit leidt tot een te hoge last in het desbetreffende boekjaar. Conform de verslaggevingsvoorschriften is dit niet toegestaan. Hierbij merken wij op dat de boeking ten laste van 2018 een bewuste keuze is geweest. In uw organisatie worden nota's die op meerdere jaren betrekking hebben geboekt ten laste van jaar waarin ze worden ontvangen. Uit onze steekproef is naar voren gekomen dat er kosten op een foutieve grootboekrekening zijn verantwoord (bij 1 van de 24 gecontroleerde facturen). Dit kan er toe leiden dat zowel uw tussentijdse informatie als de jaarrekening een onjuiste presentatie zijn van de werkelijkheid. Uit gesprekken is gebleken dat u minimaal vier keer per jaar een controle uitvoert op de juistheid van de boekingen in uw administratie. De bevindingen worden afstemt met de budgethouders. U moet de afrondende interne controle voor 2018 nog verrichten om de juistheid van de boekingen in uw administratie vast te stellen. Wij merken hierbij op dat de uitvoering van de interne controle niet wordt gedocumenteerd, waardoor deze niet reproduceerbaar is.
Advies	Voor het boekjaar 2018 adviseren wij u de boekingen in uw administratie kritisch te beoordelen, teneinde het risico op een onjuiste boeking te mitigeren. Aanvullend adviseren wij u om de periodieke controle die u uitvoert op de juistheid van de boekingen in uw administratie te documenteren. Op deze wijze is de scope van deze werkzaamheden zichtbaar en kan ook worden beoordeeld of deze periodieke beoordeling de risico's in voldoende mate afdekt.

Bevindingen en adviezen

Toelichting bevinding 3. Inkoop en aanbestedingen – niet structureel hanteren van inkoopplannen

Bevinding	Wij hebben vastgesteld dat het inkoop- en aanbestedingsbeleid voorschrijft dat voor elke inkoopopdracht een inkoopplan moet worden opgesteld. Uit het gesprek met uw organisatie is gebleken dat een inkoopplan alleen voor Europese aanbestedingen wordt opgesteld, en niet voor de overige inkopen. Dit leidt er ook toe dat de vooraf ingeschatte opdrachtwaarde en de onderbouwing van de gekozen aanbestedings-procedure onvoldoende worden gedocumenteerd. Hierdoor loopt u het risico dat de opdrachten die de Europese aanbestedingsgrens overschrijden te laat worden gesignaleerd, waardoor deze als onrechtmatig moeten worden aangemerkt. Wel dient hierbij te worden opgemerkt dat uw organisatie vanaf 2018 gebruikmaakt van een volledig contracten-register, waarin alle contracten en de bijbehorende stukken met betrekking tot de inkoop worden opgenomen. Dit dient als een beheersmaatregel om de rechtmatigheid van de inkopen te waarborgen.
Advies	Wij adviseren u: 1. Het vastgestelde inkoop- en aanbestedingsbeleid na te leven en voor alle inkoopopdrachten een inkoopplan te schrijven. Dit waarborgt dat de juiste inkoopkosten geraamd worden en dat vervolgens de juiste inkoopprocedure wordt gevolgd. 2. In de nota inkoop- en aanbestedingsbeleid een drempelwaarde op te nemen waarboven het verplichte gebruik van het inkoopplan wordt afgedwongen.

Bevindingen en adviezen

Toelichting bevinding 4. Memorialen – geen periodieke zichtbare controle en missen van deugdelijke onderbouwing

Bevinding	Wij hebben vastgesteld dat memoriaalboekingen niet worden gecontroleerd voordat deze worden doorgeboekt in uw administratie. Tijdens de controle hebben wij vastgesteld dat er nog geen interne controles hadden plaatsgevonden en dat de memorialen onvoldoende onderbouwd waren. Dit houdt een verhoogd risico in op fouten in uw administratie, aangezien middels memoriaalboekingen de reguliere procedures van uw organisatie kunnen worden doorbroken. Wel moet hierbij worden opgemerkt dat de memorialen die tot op heden waren geboekt slechts gering van omvang waren en dat het voornamelijk standaardboekingen betrof.
Advies	Wij adviseren u om bij het inboeken van een memoriaal een zichtbare interne controle uit te voeren, voordat deze in de administratie wordt verwerkt. Hiermee waarborgt u dat er enkel mutaties in de administratie worden doorgevoerd die door een daartoe bevoegde medewerker zijn geautoriseerd. Daarnaast moeten de memorialen voorzien zijn van voldoende onderbouwing, zodat blijkt waarom de memoriaal-boeking is doorgevoerd. Op basis hiervan kan de medewerker die is belast met de interne controle op de juiste wijze vaststellen of de boeking correct is doorgevoerd.

Bevindingen en adviezen

Toelichting bevinding 5. Interne controle op toepassing uitsluitings- en vrijstellingscode

Bevinding	Tijdens onze interim-controle hebben wij kennisgenomen van de rapportage inzake de interne controle op de juiste toepassing van de uitsluitings- en de vrijstellingscode. Volgens de IC-rapportage zijn er bevindingen vastgesteld die betrekking hebben op een onjuiste toepassing van deze codes.
Advies	Uit deze controle is een aantal bevindingen naar voren gekomen dat nog moet worden opgevolgd en afgewikkeld. Deze afwikkeling moet gereed zijn voor de start van de controle van de jaarverantwoordingen 2018, om zodoende vast te stellen dat dit niet zal leiden tot een fout of onzekerheid in de jaarverantwoordingen.

Bevindingen en adviezen

Toelichting bevinding 6. Stand van zaken opvolging adviespunten n.a.v. IT-audit

Bevinding	In het kader van de jaarrekeningcontrole en de controle van de belastingsverantwoordingen 2017 heeft Deloitte Risk Advisory een IT-audit uitgevoerd. Het betreft een onderzoek naar de kwaliteit van de algemene IT-beheersmaatregelen met betrekking tot Key2GH. Naar aanleiding van de uitgevoerde IT-audit is door Deloitte Risk Advisory een Memo IT- audit FY17 uitgebracht. Hierin zijn diverse aandachtspunten en actiepunten benoemd die uw organisatie dient op te pakken om de betrouwbaarheid van de geautomatiseerde gegevensbewerking te waarborgen. Op 30 januari 2019 heeft er een update gesprek plaatsgevonden over de voortgang van de adviespunten. Hierbij is middels een vraaggesprek met uw organisatie de afwikkeling van onze adviezen besproken. Er heeft daarbij geen controle plaatsgevonden op de effectieve werking van de getroffen maatregelen en de opvolging van de adviezen.
Advies	Op basis van ons vraaggesprek hebben wij vastgesteld dat uw organisatie ten opzichte van 2017 een groot aantal aanbevelingen heeft opgepakt en verbeteringen heeft aangebracht in de belastingapplicatie. Nog niet alle adviezen zijn echter opgevolgd of ze zijn deels opgevolgd. De belangrijkste adviezen in het kader van onze controle die de aandacht verdienen, zijn: - Wij hebben vastgesteld dat uw organisatie de autorisatiematrix volledig opnieuw heeft ingericht. Op deze wijze zijn de toegang tot de applicatie en de mogelijkheden die de medewerkers hebben binnen de applicatie beter afgestemd op hun functies. De uitgangspunten die ten grondslag liggen aan de autorisatiematrix zijn echter nog niet expliciet gemaakt, en zijn ook nog niet formeel door het management vastgesteld. Wij bevelen u aan deze uitgangspunten te laten vaststellen door het management. - De aanwezigheid van superusers binnen de applicatie en de acties die zij ondernemen worden nog niet gelogd en gecontroleerd. Wij bevelen u aan deze interne controle in te voeren en te documenteren, om vast te stellen dat de mutaties van de superuser juist zijn. Reactie RBG: Het GH-PLUS wachtwoord wordt veilig opborgen in een kluis en het wachtwoord wordt op aanvraag door twee daarvoor aangewezen medewerkers ingevuld/ingelogd. Controle vindt dus plaats, maar alleen de vastlegging hiervan ontbreekt nog. Hiervoor zal voortaan een logboek worden bijgehouden.

Opvolging aanbevelingen voorgaande jaren

Bevinding	**#1 Inkopen en aanbesteding – Ontbreken crediteurenanalyse rondom EU-aanbestedingen** Ten tijde van de interim-controle in 2016 had er nog geen crediteurenanalyse met betrekking tot de juiste toepassing van de EU-aanbestedingen plaatsgevonden op het totaal van de bij de leveranciers uitstaande opdrachten. Op basis van deze crediteurenanalyse kan worden vastgesteld of de aanbestedingsrichtlijnen zijn nageleefd.
Follow-up 2018	Wij hebben vastgesteld dat deze analyse voor het boekjaar 2017 nog in onvoldoende mate is opgesteld en dat deze nog niet voldoet aan de eisen die hieraan gesteld worden. Wij adviseren u dan ook voor 2018 deze controle met meer diepgang uit te voeren en de documentatie hierbij te verbeteren.
Status 2018	**Niet opgelost**

Bevinding	**#2 Algemeen– Integriteitstoets** Wij adviseren u om een integriteitstoets uit te voeren onder de medewerkers die wonen binnen uw ‘bedieningsgebied’. Hierbij worden de aanslagen van de medewerkers gecontroleerd en wordt het betaalgedrag geëvalueerd. Door het invoeren van de integriteitstoets wordt het risico op het niet of laat ontdekken van niet-integer handelen van medewerkers gemitigeerd.
Follow-up 2018	Wij hebben vastgesteld dat dit punt is opgelost.
Status 2018	**Opgelost**

Opvolging aanbevelingen voorgaande jaren

Bevinding	**#3 Vrijstellingen– Uitvoeren zichtbare controle op de vrijstellingen** Wij adviseren u om periodiek een interne controle uit te voeren op de vrijgestelde objecten. Naar onze mening is deze controle het beste uit te voeren op mutatieoverzichten van de vrijgestelde objecten ten opzichte van de ervoor gecontroleerde periode. Op basis van deze overzichten kunt u een steekproefsgewijze controle uitvoeren op de juistheid van de opgestelde vrijstelling.
Follow-up 2018	Wij hebben vastgesteld dat dit advies in 2018 is opgevolgd. Uit deze controle zijn echter bevindingen naar voren gekomen die nog dienen te worden opgevolgd en afgewikkeld vóór de controle van de jaarverantwoordingen 2018.
Status 2018	**Opgelost**

Bevinding	**#4 Frauderisicoanalyse – Het updaten en verbeteren van de frauderisicoanalyse** Wij willen u adviseren om jaarlijks de frauderisicoanalyse te updaten, teneinde vast te stellen dat deze nog aansluit op uw huidige bedrijfsvoering en op de risico's waarmee uw organisatie te maken heeft. Daarnaast adviseren wij u om uw frauderisicoanalyse te verbeteren door hier een risicoclassificatie in aan te brengen en het restrisico te bepalen dat overblijft na de getroffen beheersmaatregelen.
Follow-up 2018	Wij hebben vastgesteld dat dit punt deels is opgevolgd. De risicoclassificatie is toegevoegd aan uw risicoanalyse. Het ontbreekt echter nog aan een analyse van het restrisico.
Status 2018	**Deels opgelost**

Actuele ontwikkelingen

Wet normering topinkomens (WNT)

Bezoldigingsnorm 2018

Voor 2018 bedraagt de algemene maximale bezoldigingsnorm voor topfunctionarissen in dienstbetrekking € 189.000 per jaar op fulltime basis.

Voor interim-topfunctionarissen geldt in 2018 als norm per maand:
- € 25.300 voor de eerste zes maanden van de functievervulling
- € 19.100 voor de volgende zes maanden

Het maximale uurtarief in 2018 bedraagt € 182.

Wijzigingen in wet- en regelgeving

Op 1 juli 2017 is de Evaluatiewet WNT in werking getreden. De bepalingen uit deze Evaluatiewet verschillen wat betreft het moment van inwerkingtreding. Per 1 januari 2018 geldt onder andere:
- WNT-organisaties zijn verplicht om hun WNT-verantwoording op internet te publiceren voor een periode van ten minste zeven jaar. Dat mag als onderdeel van de jaarrekening of als apart document. De gegevens moeten vrij toegankelijk en eenvoudig te vinden zijn.
- Eenieder die de functie van topfunctionaris voor een periode van ten minste twaalf kalendermaanden heeft vervuld en daarna bij dezelfde rechtspersoon of instelling in dienstverband een andere functie vervult, wordt voor een periode van vier jaar gezien als topfunctionaris. Dit betekent dat zowel de normering als de publicatieplicht van toepassing blijft. Deze aanscherping geldt alleen voor dienstverbanden die worden aangegaan na 1 januari 2018, alsmede voor dienstverbanden die na 1 januari 2018 worden verlengd.
- Het begrip 'gewezen topfunctionaris' is vervallen. In de WNT-verantwoording 2018 worden geen gewezen topfunctionarissen meer verantwoord.

Vanaf 1 januari 2018 is de anticumulatiebepaling uitgebreid. Als een topfunctionaris voor verschillende niet-gelieerde WNT-instellingen in dienstbetrekking als topfunctionaris werkt, mag de som van de bezoldigingen uit de verschillende functies niet meer bedragen dan de algemene bezoldigingsnorm van € 187.000 (2018). De anticumulatie-bepaling geldt niet voor een functie als toezichthouder.

Een verplichte transitievergoeding ingevolge artikel 7:673 BW is geen beëindigingsvergoeding in de zin van de WNT. Dit betreft namelijk uitsluitend een transitievergoeding die volgt uit voornoemd artikel. Transitievergoedingen die niet op grond van artikel 7:673 BW worden uitbetaald, maar worden verkregen op grond van een vaststellings- of beëindigingsovereenkomst, moeten namelijk wel worden aangemerkt als beëindigingsvergoeding in de zin van de WNT.

Evaluatie werkkostenregeling (WKR)

Op 23 maart 2018 is het rapport Evaluatie werking werkkosten-regeling aangeboden aan de Tweede Kamer. Het kabinet ziet na de evaluatie geen aanleiding de regeling grondig aan te passen. Wel geeft het oplossingen voor enkele knelpunten binnen de WKR, zoals het noodzakelijkheidscriterium, niet-zakelijke lunches op de werkplek, en de wijze van aanwijzen van gerichte vrijstellingen. Voor de belangrijkste knelpunten die wij in de praktijk zien (onzuivere boekingsgang en onvoldoende onderbouwing van de gerichte vrijstellingen), blijft het essentieel om dit in de processen van de organisatie te borgen en hier periodiek op te monitoren.

Wilt u weten of uw organisatie de werkkostenregeling fiscaal optimaal en correct heeft ingericht? Neem dan gerust contact met ons op. Wij bieden u inzicht door het trekken van een steekproef, met onze Werkkosten Monitoring Tool, of met de WKR Analytics tool.

Actuele ontwikkelingen

Wet deregulering beoordeling arbeidsrelaties (Wet DBA)

Het kabinet heeft in het regeerakkoord maatregelen aangekondigd om vooral aan de onderkant van de arbeidsmarkt schijnzelfstandigheid en concurrentie op arbeidsvoorwaarden tegen te gaan. Deze maatregelen beogen bovendien zowel zelfstandigen als hun opdrachtgevers de zekerheid te bieden dat geen sprake is van een dienstbetrekking. Het kabinet zet de komende maanden in op een aantal vervolgacties die het wetgevingsproces verder zullen brengen. Het kabinet is voornemens om de Tweede Kamer in het najaar van 2018 nader te informeren over de uitwerking van de voorgestelde maatregelen.

De handhaving van de Wet DBA is tot in ieder geval 1 januari 2020 opgeschort, met uitzondering van 'kwaadwillenden'. Zorg er daarom voor dat u goed in beeld heeft met welke ZZP'ers er wordt gewerkt, en dat u waar nodig nieuwe afspraken maakt, zodat de Belastingdienst niet kan stellen dat er sprake is van 'kwaadwillendheid'.

Opdrachtgevers en opdrachtnemers die *feitelijk* overeenkomstig een goedgekeurde modelovereenkomst werken, hebben de zekerheid dat een naheffingsaanslag loonheffingen achterwege blijft bij de opdrachtgever.

Wet Ketenaansprakelijkheid (WKA)

Aannemers kunnen aansprakelijk worden gesteld voor de niet afgedragen loonheffingen die onderaannemers verschuldigd zijn in verband met het verrichten van werkzaamheden door hun werknemers inzake het aangenomen werk. Ook kunnen zogenoemde 'eigenbouwers' met aannemers worden gelijkgesteld. Niet iedere organisatie is 'eigenbouwer'. De organisatie moet bijvoorbeeld zelf de algehele leiding over de bouwwerkzaamheden voeren of de kennis in huis hebben om het project zelf te kunnen uitvoeren. Daar komt nog bij dat het 'eigenbouwerschap' zich alleen kan voordoen bij opdrachten vanuit de ondernemerssfeer van de organisatie.

Indien en voor zover bij de uitvoering van opdrachten persoons-gegevens worden verwerkt (opslaan, aanpassen, doorzenden, etc.), dient de uitwisseling en (verdere) verwerking ervan plaats te vinden in overeenstemming met de AVG. Organisaties worden onder de AVG verplicht zorgvuldig om te gaan met persoonsgegevens. Het vaststellen en beheersen van mogelijke WKA-risico's is complex. Voldoende kennis van de WKA en de daarmee samenhangende regelgeving is dan ook onontbeerlijk. Twijfelt u eraan of u in staat bent het WKA-risico adequaat te beoordelen? Neem dan gerust contact met ons op.

Actuele ontwikkelingen

Transparantie over duurzaamheidsthema's

Transparantie ten aanzien van de prestaties op het gebied van duurzaamheid wordt steeds belangrijker in het maatschappelijk verkeer. Dit is ook te zien in de toenemende nationale en internationale wet- en regelgeving omtrent het rapporteren over Environmental, Social en Governance (ESG-)thema's. Een voorbeeld hiervan is de in de Nederlandse regelgeving opgenomen EU Directive 2014/95 inzake de niet-financiële rapportage. Deze richtlijn brengt voor Organisaties van Openbaar Belang reeds verplichtingen met zich mee om te rapporteren over een aantal prestaties met betrekking tot het milieu, sociale verantwoordelijkheid en integriteit. Onze verwachting is dat dit voor gemeenschappelijke regelingen de komende jaren eveneens zal worden aangescherpt.

Daarnaast zien wij een verhoogde aandacht voor ESG-thema's (ook 'sustainablity-thema's' genoemd) bij burgers en andere stakeholders ontstaan, waarbij van gemeenschappelijke regelingen wordt verlangd dat zij inzicht te verschaffen in hun rol met betrekking tot bijvoorbeeld de energietransitie.

Hoewel er op dit moment nog geen wettelijke verplichting voor gemeenschappelijke regelingen geldt om te rapporteren over deze thema's en om daar assurance bij te verkrijgen, raden wij u aan om uw stakeholderdialoog met betrekking tot deze gebieden te gebruiken om relevante thema's te identificeren. Het bepalen van heldere doelstellingen en het daarop sturen en rapporteren versterken uw maatschappelijke functie en relaties. Een veel gehanteerde methodiek hierbij is het raamwerk van de Sustainable Developments Goals van de VN.

Duurzame inzetbaarheid

Het onderwerp 'duurzame inzetbaarheid' is goed bespreekbaar te maken aan de hand van vier pijlers:
- In-, door- en uitstroom
- Beloning
- Preventie en verzuim
- Financiën

Aan de hand van deze pijlers komt niet alleen het economisch perspectief aan bod (met als eye-opener de kosten van een zieke werknemer), maar ook het ontwikkelperspectief.

In de praktijk zien wij dat organisaties die een beleid hebben ontwikkeld tot vergroting van de duurzame inzetbaarheid moeite hebben de balans te vinden tussen de benodigde acties op de diverse doelgroepen binnen de organisatie en de kosten. Het ontbreken van draagvlak en het niet-meetbaar maken van de resultaten leiden tot onzekerheid over de juistheid van de gekozen aanpak. Met het inzetten van een multidisciplinair team helpt Deloitte werkgevers om het gewenste resultaat te behalen.

Actuele ontwikkelingen

Cybersecurity

Cyber is een onlosmakelijk onderdeel geworden van de samenleving. Dagelijks werken we met digitale oplossingen, zowel privé als zakelijk. Door gebruik van het internet, bedrijfsnetwerken en -applicaties hebben alle organisaties, ongeacht hun omvang, te maken met aan cyber gerelateerde risico's, zoals cybercrime. Als cyberrisico's zich voordoen, kunnen ze een forse impact hebben op de financiële systemen, de interne beheersing en daarmee op de jaarrekening-controle.

De maatschappij verwacht van overheden een betrouwbaar IT-systeem, dat cyberaanvallen detecteert en voorkomt of afwendt. Het voldoen aan deze publieke verwachting vergt van u passende maatregelen. De technische complexiteit en snelheid van IT-ontwikkelingen vormen extra redenen om dit onderwerp periodiek te agenderen in uw vergaderingen. 'Cyber' vormt inmiddels ook een vast onderwerp in de accountantscontrole. Kortheidshalve verwijzen wij naar de publicatie "*Van hype naar aanpak"*, de publieke managementletter over cybersecurity.

Wij willen u met betrekking tot cybersecurity het volgende meegeven:

- Verricht periodiek een cyberrisicoanalyse, als vast onderdeel van het interne-controlesysteem en het risicomanagement.
- Wees als bestuurder kritisch op cybersecurity en op de wijze waarop de organisatie hiermee omgaat.
- Breng in kaart wat de belangrijkste te beveiligen gegevens zijn voor uw organisatie en stel vast of deze gegevens voldoende beveiligd zijn voor interne en externe belanghebbenden.
- Prioriteer de maatregelen daarbij op basis van de waarde en het risico dat daarmee gepaard kan gaan.
- Cultuur en gedrag van mensen zijn belangrijke factoren in het kader van cybersecurity. Zorg daarom voor bewustwording in uw organisatie.

Cybercrime is anno 2018 een inherent risico voor iedere organisatie. Het accepteren hiervan maakt deel uit van de bewustwording in uw organisatie, leidend tot een aanpak in het kader van cybersecurity.

Actuele ontwikkelingen

De Algemene Verordening Gegevensbescherming (AVG)

Sinds 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. De nadruk ligt nu (veel meer dan voorheen bij de Wet Bescherming Persoonsgegevens (Wbp) op de verantwoordelijkheid van organisaties om zorgvuldig en bewust gebruik te maken van persoonsgegevens. Organisaties zijn verantwoordelijk voor de naleving van alle bepalingen uit de AVG en zij moeten kunnen aantonen dat zij hier actief mee bezig zijn.

Onder andere de volgende wijzigingen zijn van kracht geworden:

- Organisaties moeten een register bijhouden waaruit blijkt welke persoonsgegevens voor welke doeleinden worden bijgehouden, hoe ze zijn opgeslagen en beveiligd, voor welke termijn ze zijn opgeslagen en of ze met derden worden gedeeld (en zo ja, met welke). Een dergelijk register verplicht organisaties tot het geven van inzicht in het antwoord op de vraag waarvoor de persoons-gegevens worden gebruikt, maar biedt ook een uitgangspunt voor een gedegen privacy-huishouding.

- Mocht daarnaast blijken dat een proces mogelijk een hoog risico oplevert voor individuen, dan is een impact assessment verplicht.

- Daarnaast heeft het beginsel van gegevensbescherming door ontwerp (*privacy by design*) en door standaardinstellingen (*privacy by default*) zijn intrede gedaan.

Betrokken individuen hebben meer rechten gekregen. Naast bijvoorbeeld het reeds bestaande recht op inzicht en het recht om vergeten te worden, is het ook mogelijk om te vragen gegevens over te dragen aan een andere organisatie. Gelet op de toenemende bekendheid van deze rechten, is de verwachting dat er in de toekomst steeds meer gebruikgemaakt zal worden van deze rechten, des te meer nu de AVG de mogelijkheid heeft weggenomen om een monetaire barrière op te werpen om de uitoefening van deze rechten te voorkomen.

Wij hebben begrepen dat uw organisatie al verschillende maatregelen op het gebied van dataprivacy heeft genomen. Uw organisatie is volledig zelf verantwoordelijk voor het voldoen aan wet- en regel-geving, waaronder ook de nieuwe AVG valt.

Wij adviseren uw organisatie een analyse uit te voeren om inzichtelijk te krijgen of in alle opzichten aan de van toepassing zijnde eisen ten aanzien van de AVG wordt voldaan en of de verantwoordelijkheden op het juiste niveau in de organisatie zijn belegd. Een risico-en-controle-matrix, voor zover nog niet gerealiseerd, kan een belangrijke bijdrage leveren aan het proces van het blijvend monitoren in hoeverre de organisatie compliant is met de AVG. Daarnaast benadrukken wij het belang van effectieve IT General Controls rondom uw kritische systemen, om een betrouwbare verwerking van persoonsgegevens te waarborgen.

Voor verdere details rondom de nieuwe privacywetgeving verwijzen wij naar de als bijlage A opgenomen toelichting AVG.

Bijlage

Bijlage A - Toelichting AVG

De Algemene Verordening Gegevensbescherming (AVG)
Sinds 25 mei 2018 kan iedere natuurlijk persoon binnen de EU organisaties aanspreken op het niet nakomen van de AVG. De wetgeving wil het transparant, het zorgvuldig en het bewust gebruik van persoonsgegevens bevorderen.

Toepassing
De AVG is van toepassing op elke organisatie in de Europese Unie die persoonsgegevens verwerkt. Daarnaast gaat de wetgeving ook gelden voor organisaties die diensten en of goederen aanbieden aan individuen buiten de Europese Unie, al dan niet om iets. Mocht een organisatie het gedrag van individuen monitoren voor zover dit gedrag plaatsvindt op het grondgebied van de EU, dan zal de organisatie ook moeten voldoen aan de AVG. De AVG heeft dus een reikwijdte die verder gaat dan slechts de grenzen van de EU.

Rechten van individuen
De AVG maakt het voor individuen mogelijk om kosteloos inzicht te krijgen in de persoonsgegevens die een organisatie van hem/haar verwerkt. In bepaalde gevallen is het mogelijk voor een individu om gegevens te wijzingen, te laten verwijderen, een verzoek in te dienen om verdere verwerking te blokkeren en zelfs om te vragen of gegevens overgedragen kunnen worden naar een andere partij.

Wat er gelijk is gebleven
Veel van de reeds bestaande principes zijn gelijk gebleven. Zo mogen gegevens alleen voor een specifiek doel worden verwerkt, moet er een wettelijke basis bestaan voor het gebruik van die gegevens, en mogen zij niet verder verwerkt worden, indien dit niet verenigbaar is met het oorspronkelijke doel. Ook onder de AVG blijft de plicht bestaan om datalekken te melden binnen 72 uur.

Verwerkingsverantwoordelijkheid
Wellicht de grootste verandering is het beginsel van de verwerkings-verantwoordelijkheid. Organisaties zijn verantwoordelijk voor de naleving van alle bepalingen uit de AVG, en moeten kunnen aantonen dat zij hier actief mee bezig zijn. Dit betekent dat de AVG een hoge mate van volwassenheid en documentatie verlangt. Zonder het actief documenteren van genomen maatregelen en de afwegingen die zijn gemaakt om tot die maatregelen te komen, wordt het lastig voor organisaties om aan te tonen dat zij actief bezig zijn geweest met deze wetgeving.

Verwerkingsregister en gegevensbescherming door ontwerp en standaardinstellingen
Organisaties zijn verplicht om een register bij te houden, waarin zij hun verwerkingsactiviteiten registreren, met daarbij aanvullende informatie, zoals bewaartermijnen en genomen beveiligings-maatregelen. Daarnaast moeten alle processen binnen de organisatie ontworpen worden met de bescherming van persoonsgegevens als centraal uitgangspunt, het zogenoemde *'gegevensbescherming door ontwerp'* (privacy by design). Daarbij moeten deze processen standaard de voor het individu minst indringende instellingen hebben, het zogenoemde *'gegevensbescherming door standaardinstellingen'* (privacy by default). Technische en organisatorische maatregelen moeten daarom geïmplementeerd zijn in en rondom het gehele proces van het verwerken van persoonsgegevens (art. 25 AVG). Al deze maatregelen hebben als doel het vertrouwen van het individu in de digitale wereld te vergroten.

Bijlage A - Toelichting AVG

Impact assessment
Voor iedere nieuwe gegevensverwerking dient de verantwoordelijke gegevensverwerker een impact-analyse uit te voeren indien de verwerking een hoog risico oplevert voor de bescherming van de persoonsgegevens van de betrokkene. Het individu dient hierbij als uitgangspunt. Zo'n impact assessment moet in ieder geval plaatsvinden indien een organisatie systematisch individuen monitort of op grootschalig niveau gevoelige gegevens verwerkt. Hierbij zal het criterium 'grootschalig' worden ingevuld aan de hand van zowel de hoeveelheid gegevens als de hoeveelheid betrokkenen.

Toezichthoudende autoriteit
In Nederland is de Autoriteit Persoonsgegevens (voorheen: College Bescherming Persoonsgegevens) de toezichthoudende autoriteit die bevoegd is om handhavend op te treden in het geval de AVG niet wordt nageleefd. De Autoriteit Persoonsgegevens heeft daarnaast als taak om praktische informatie te verstrekken over de AVG en om leading practices te identificeren en te verspreiden. Mocht dit nodig zijn, dan heeft de toezichthouder de bevoegdheid om een boete op te leggen als blijkt dat een organisatie zich niet heeft gehouden aan de AVG. Deze boetes kunnen oplopen tot maximaal € 20 miljoen of 4% van de wereldwijde omzet van het voorgaande jaar.

Lidstatelijke maatregelen
Hoewel de AVG een uniforme set regels beoogt te creëren voor alle landen in Europese Unie, zullen lidstaten in bepaalde gevallen bevoegd zijn om aanvullende regels op te stellen voor het beschermen van persoonsgegevens. Hoewel voor multinationals in grote lijnen een uniforme implementatie van de AVG mogelijk is, zal er daarom toch ook naar nationale bepalingen gekeken moeten worden bij het uitvoeren van een privacyprogramma.

Beveiliging van persoonsgegevens
Naast het zorgvuldig verzamelen van persoonsgegevens moet een organisatie de persoonsgegevens ook op een juiste en passende manier organisatorisch en technisch beveiligen. Dit houdt onder andere in dat de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens geborgd worden. Het feit dat die gegevens niet alleen technisch beveiligd moeten worden maar ook organisatorisch, benadrukt dat het beschermen van gegevens ook offline moet gebeuren.

Functionaris voor de gegevensbescherming
De AVG dwingt af dat sommige organisaties een functionaris ten behoeve van gegevensbescherming aanstellen. Deze functie dient zich namens de organisatie onder andere bezig te houden met het toepassen en naleven van de AVG en het interne dataprivacybeleid.

De verplichting om een functionaris voor de gegevensbescherming in te stellen geldt in ieder geval voor overheidsinstellingen. Voor andere organisaties is het afhankelijk van de omvang van de organisatie en/of de hoeveelheid en typen persoonsgegevens die worden verwerkt, of een functionaris gegevensbescherming moet zijn aangesteld voor het toepassen en naleven van de AVG en het melden van datalekken bij de toezichthoudende autoriteit.

Deloitte.