



ICT en het kleine accountantskantoor



Oktober 2018

© 2018 Koninklijke NBA

Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt in enige vorm of op enige wijze, hetzij door middel van druk, fotokopieën, microfilm of op welke andere wijze dan ook, zonder voorafgaande toestemming van de NBA.

Disclaimer

Deze brochure is zo zorgvuldig mogelijk samengesteld. De NBA is echter niet aansprakelijk voor eventuele onjuistheden. De NBA heeft er voor gekozen een maximaal leesbare brochure op te stellen.

Oktober 2018

ICT en het kleine accountantskantoor

Volgens de VGBA (artikel 16 inzake vertrouwelijkheid) bent u verplicht om gegevens met een vertrouwelijk karakter geheim te houden. Dat betekent niet alleen dat u anderen niet actief kennis mag laten nemen van deze gegevens. Het betekent ook dat uw kantoor zodanig moet zijn ingericht dat derden niet zomaar bij vertrouwelijke gegevens kunnen komen. U moet zo goed mogelijk voorkomen dat uw ICT-systeem gehackt wordt. En wanneer er toch een inbreuk is, dat u dat ook ontdekt.

Daarnaast stelt de Algemene verordening gegevensbescherming (AVG) niet alleen 'papierse eisen' zoals verwerkersovereenkomsten, registers, etc., maar stelt ook eisen aan de 'basis hygiëne' van de kantoorautomatisering. De AVG heeft het over technische en organisatorische maatregelen, rekening houdend met de stand der techniek, de uitvoeringskosten en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen.

Tenslotte is het kwijtraken van klantgegevens en mogelijke publicaties hierover niet bevorderend voor uw bedrijfsvoering.

Er zijn geen concrete regels voor de automatisering van een accountantskantoor. Om toch wat handvatten te geven, geven we in deze brochure een aantal zaken weer waaraan u kunt denken.

1 De interne automatisering

In elk accountantskantoor dat niet volledig online werkt (bijvoorbeeld op premise of met virtual machine) zullen meerdere computers aanwezig zijn die met elkaar verbonden zijn via een server of op een andere manier. Het is verstandig om het aantal externe verbindingen die in dit systeem kunnen zoveel als mogelijk te beperken. Zo moet voorkomen worden dat een buitenstaander, bijvoorbeeld het ICT-ondersteuningsbedrijf, willekeurig in uw systemen kan. Zet bij een op afstand op te lossen probleem een tijdelijke beveiligde verbinding op en kijk mee op het scherm, wat de ICT'er doet. Ook moeten er goede afspraken met ICT-bedrijven gemaakt worden. En het is natuurlijk heel belangrijk dat u een professionele ter zake kundige dienstverlener heeft. Het kan niet zo zijn dat een familielid of buurman het systeem 'even' voor u opzet.

Om u te helpen vindt u in de Privacy toolkit op mijnba.nl een basischecklist automatisering, waar met name naar organisatorische maatregelen verwezen wordt. U treft hier onder meer tips aan over wachtwoorden, updates, etc.

www.nba.nl/avg-basischecklist-automatisering/

Online softwarepakketten

Vrijwel elk accountantskantoor maakt gebruik van online softwarepakketten. Soms wordt er te gemakkelijk aangenomen dat de leverancier er wel voor zorgt dat een dergelijk pakket veilig is. Dat is echter niet altijd waar. U moet zich er zelf van overtuigen dat het pakket veilig is. Dat kan bijvoorbeeld doordat de leverancier een keurmerk van Zeker-online heeft. (www.zeker-online.nl) Ook kan het zijn dat de leverancier een passende audit heeft laten uitvoeren en u het certificaat overhandigt.

Twee factor authenticatie

Wanneer u of uw medewerkers van buiten kunnen inloggen gebruik dan twee factor authenticatie. Dit houdt in dat niet alleen gebruikersnaam/ wachtwoord gebruikt wordt, maar daarnaast ook gebruik wordt gemaakt van een token, usb stick of telefonische code. Wanneer u bijzondere persoonsgegevens verwerkt (bijvoorbeeld religieuze of medische gegevens) is twee factor authenticatie zelfs verplicht.

2 De website

Veel accountantskantoren gebruiken nog onbeveiligde websites. Dit is te zien aan het begin van de adresregel; http://. Bij een beveiligde website begint de adresregel met https:// en staat er ook een slotje in de adresbalk. Wanneer u via een beveiligde website gegevens uitwisselt zijn deze versleuteld en daarmee onleesbaar tijdens het versturen. Hackers hebben er daardoor niets aan. Om dit te bereiken dient u een zogenaamd SSL-certificaat te installeren.

Naast de veiligheid is het ook beter voor de uitstraling. Wanneer een (potentiële) klant op een onbeveiligde website komt, kan hij een waarschuwing op zijn scherm zien. Daarnaast worden beveiligde websites bij bijvoorbeeld Google hoger gerankt dan onbeveiligde.

3 E-mail verkeer

Tegenwoordig worden veel producten naar de klanten gemaild. Het betreft vaak (concept) jaarrekeningen, aangiften, loonstroken, etc. Wanneer dit onbeveiligd gebeurt, loopt u als accountant grote risico's, waaronder het verzenden naar de verkeerde persoon, hacken en/of manipulatie van gegevens. Het is in elk geval niet verstandig om een door de accountant ondertekende accountantsverklaring te scannen en per onbeveiligde mail te versturen.

Een eerste stap kan zijn om in elk geval de te verzenden documenten te beveiligen met een wachtwoord. Dit wachtwoord moet natuurlijk separaat (bijvoorbeeld per post) naar de cliënt worden verzonden. Dit mag geen standaard wachtwoord zijn, maar moet per cliënt verschillen. Als een verkeerde ontvanger geen wachtwoord heeft, zal deze het document niet met normale middelen kunnen openen en hoeft er geen sprake te zijn van een datalek.

Een stap verder is een beveiligde e-mailverbinding per klant, waarbij versleutelde berichten worden verzonden. Dit betekent dat de afzender en de ontvanger hun digitale id ofwel openbare sleutel van het beveiligingscertificaat uitwisselen. Het versleutelen kan daarna in bijvoorbeeld outlook plaatsvinden.

Een PDF

In plaats van het versturen van een 'nat' ondertekende pdf-jaarrekening, verdient het aanbeveling om deze ook met een PKloverheid beroepscertificaat ondertekenen. Er staat dan vast dat u het ondertekend heeft en dat u accountant bent. Met dit beroepscertificaat kunt u bijvoorbeeld ook e-mails ondertekenen.

4 De Cloud

Steeds meer toepassingen vinden niet meer plaats op de systemen van het accountantskantoor maar vinden "ergens" in de Cloud plaats. Voorbeelden zijn online-software, back-ups en opties om bestanden te delen. Een goede cloudoplossing is gemakkelijk schaalbaar en beperkt de noodzaak voor beveiligingsmaatregelen op het eigen kantoor. Natuurlijk zijn er ook hier belangrijke aandachtspunten, zoals;

- Voldoen aan de AVG (kan ik dit aantonen?)
- Afhankelijkheid van de aanbieder (kan ik de data meenemen als ik weg ga?)
- Bedrijfszekerheid (is het risico beperkt dat het systeem uitvalt of de leverancier helemaal verdwijnt?)
- Maatwerk (is het systeem aan te passen aan de eisen van het kantoor?)

Wij adviseren accountants voorzichtig te zijn met aanbieders die databestanden voor u opslaan en delen. Voor de vakantiefoto's kan het systeem voldoende beveiligd zijn, maar het kan zijn dat uw klantgegevens in landen terecht komen, waar

ze gevaar lopen dan wel eenvoudig voor derden toegankelijk zijn. Zie ook de NBA-flyer over cloud-computing. www.nba.nl/flyer-cloud-computing

5 Klantenportaal

Een veilig alternatief voor de communicatie met cliënten en medewerkers is een klantenportaal. U zet stukken klaar in het portaal en de klant kan deze overal ter wereld bekijken en zo nodig goedkeuren. De klant drukt als het ware op de knop voor verzending naar belastingdienst of Kamer van Koophandel. De goede portaalleverancier zorgt ervoor dat dit alles veilig gebeurt zodat de hackkansen minimaal zijn. Ook het koppelen van cloudapplicaties kan vaak eenvoudig en veilig plaats vinden. Daarnaast is er vaak een mogelijkheid voor single sign-in, zodat klanten en/of medewerkers na een keer inloggen bij diverse applicaties kunnen.

Wanneer een kantoor wil starten met een klantenportaal is het wel zaak om te zorgen dat dit portaal bij het kantoor past en de gekochte onderdelen ook worden gebruikt. Het is dus belangrijk om tevoren vast te stellen wat u nu en later met het portaal wil bereiken en te zorgen dat het portaal aansluit bij de eigen werkprocessen.

Er zijn portaalsystemen die aan een softwarepakket gekoppeld zijn en losse systemen die met diverse pakketten en uitvragende partijen kunnen werken.

Koninklijke Nederlandse
Beroepsorganisatie
van Accountants



Antonio Vivaldistraat 2 - 8
1083 HP Amsterdam
Postbus 7984
1008 AD Amsterdam

T 020 301 03 01
E nba@nba.nl
I www.nba.nl