Informatiebeveiligingsbeleid van DH Accountants en Belastingadviseurs B.V. (KvK-nr. 09095268)

Inleiding

Dit artikel bevat ons informatiebeveiligingsbeleid. Cybercrime neemt hand over hand toe en is helaas niet meer weg te denken uit onze maatschappij. Het risico om slachtoffer te worden, neemt steeds verder toe. Het betreft criminaliteit met ICT als middel en doelwit. Om slachtoffer van cybercrime te worden, is niet eens een computer of internetaansluiting nodig. Zo bevatten de meeste telefoons en bankpassen computerchips, die kunnen worden gemanipuleerd door cybercriminelen.

Ook als accountantskantoor worden wij geconfronteerd met het toenemende risico van cybercrime en de mogelijke gevolgen daarvan voor onze bedrijfsvoering en reputatie als professioneel dienstverlener. Ons informatiebeveiligingsbeleid, privacybeleid en de maatregelen die uit dit beleid voortvloeien in ons stelsel van kwaliteitsbeheersing, hebben tot doel om de schade te voorkomen dan wel te beperken indien wij slachtoffer worden van cybercrime.

Als accountantskantoor maken wij gebruik van gegevens van onze cliënten en verwerken wij persoonsgegevens. Bedrijfs- en persoonsgegevens kunnen economisch gezien een grote waarde vertegenwoordigen. Het verlies of bekend worden van deze gegevens kan niet alleen grote bedrijfsschade opleveren voor onze cliënten maar ook voor ons als professioneel dienstverlener. Dit betekent dat de bescherming van bedrijfs- en cliëntgegevens een essentiële voorwaarde is voor de ‘Licence to Operate’ van ons als accountantskantoor. Goede informatiebeveiliging is in dit kader essentieel.

Een goede informatiebeveiliging is ook nodig om te kunnen voldoen aan de eisen die vanuit de Algemene verordening gegevensbescherming (AVG) aan ons kantoor worden gesteld. Uitgangspunt voor ons kantoor hierbij is het privacybeleid zoals tevens in deze sectie is opgenomen.

Aanpak informatiebeveiliging

Informatiebeveiliging omvat het geheel aan maatregelen waar wij onze informatie beveiligen. Het gaat daarbij om alle informatie die wij verwerken, zowel digitaal als niet digitaal. Als kantoor hebben wij niet alleen informatie nodig om onze bedrijfsprocessen uit te voeren, maar ook om de interne bedrijfsvoering bij te sturen en strategische beslissingen te nemen. Informatiebeveiliging richt zich op het waarborgen van de betrouwbaarheid, bestaande uit integriteit, beschikbaarheid en vertrouwelijkheid van processen en data.

Naast de drie bovengenoemde aspecten, die betrekking hebben op de informatie en de verwerking ervan, onderkennen wij nog een vierde en een vijfde aspect:

1. Beheersbaarheid: de beheersbaarheid is de mate waarin de organisatie, het systeem of een proces kan worden aangestuurd en/of bijgestuurd, zodat het object bij voortduring aan de daaraan gestelde eisen voldoet of kan voldoen. Beheersbaarheid is de verantwoordelijkheid van de vennoten;
2. Controleerbaarheid: de controleerbaarheid betreft de mogelijkheid om met voldoende zekerheid (achteraf) vast te kunnen stellen of wordt/is voldaan aan de eisen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Informatiebeveiliging richt zich op de organisatie, de systemen en de processen met als doel deze, alsmede de verwerkte en opgeslagen data te beschermen tegen dreigingen die de integriteit, beschikbaarheid en vertrouwelijkheid kunnen aantasten, alsmede compliance.

Informatiebeveiliging is een verantwoordelijkheid van de vennoten waarin afwegingen worden gemaakt tussen de te bereiken doelen en 'risk appetite' (welk risico willen wij lopen) versus de te nemen maatregelen. Dit betreft een risk based benadering. De dwingende bepalingen in de AVG maken echter dat wij als accountantskantoor beperkt worden in onze keuzemogelijkheden, omdat wij passende maatregelen moeten treffen om bijvoorbeeld de rechten van betrokkenen te kunnen waarborgen.

Risicoanalyse versus baseline benadering

Om passende beveiligingsmaatregelen te kunnen nemen is het van belang zicht te hebben op welke gebieden ons kantoor de grootste risico's loopt. Hierbij hebben wij de keuze om een risicoanalyse uit te voeren dan wel voor een zogenaamde baseline benadering te kiezen. Ons kantoor heeft ervoor gekozen om de baseline benadering toe te passen omdat het uitvoeren van een risicoanalyse doorgaans veel tijd in beslag neemt en daarmee een (te) grote druk legt op ons kantoor en onze medewerkers. Bij deze baseline benadering heeft ons kantoor een basisbeveiligingsniveau ingevoerd. Vervolgens wordt bepaald welke aanvullende maatregelen noodzakelijk zijn waarbij jaarlijkse evaluatie plaatsvindt. In ons stelsel van kwaliteitsbeheersing zijn de middelen opgenomen om concreet invulling te geven aan deze jaarlijkse evaluatie en de vastlegging daarvan.

Uitgangspunten beveiligingsbeleid

Bij de beveiligingsmaatregelen hanteren wij de volgende uitgangspunten:

Het maximeren van de eigen regie

- Wij nemen het initiatief door verantwoordelijkheden binnen ons kantoor (vennoten, kwaliteitsbepaler) en met partijen (cliënten en verwerkers) expliciet te maken, mede door middel van ons privacy statement;
- Wij inventariseren periodiek de gevolgen van de AVG voor ons kantoor;
- Wij leggen afspraken over gegevens, verwerkingen en verantwoordelijkheden vast in onder andere registers van verwerkingsactiviteiten en verwerkersovereenkomsten.

Het maximeren van beheerste flexibiliteit

- Wij vertalen de flexibiliteit van onze dienstverlening naar cliënten in beheersbare bedrijfsvoering door maximale automatisering;
- Wij hebben cliëntoplossingen maximaal gestandaardiseerd met behoud van keuzevrijheden.

Het minimaliseren van de complexiteit

- Wij passen het 'Need to know' principe toe voor alle partijen (medewerkers, cliënten, dienstverleners) in het verlenen van bevoegdheden. Hierbij voorkomen wij zoveel als mogelijk overtollige of tegenstrijdige bevoegdheden die tot inbreuken kunnen leiden;
- Wij reduceren de complexiteit in de informatievoorziening door de beste oplossing voor het geheel te kiezen en niet alleen de beste deeloplossing. Het geheel van de beste deeloplossingen kan voor een hoge mate van complexiteit en dus voor management (lees: privacy) problemen zorgen;

- Wij zijn selectief in creatieve tijdelijke oplossingen. Deze oplossingen kunnen zeer structurele vormen aannemen met alle risico's van dien;
- Wij minimaliseren de opgeslagen persoonsgegevens omdat persoonsgegevens alleen mogen worden verwerkt als er een grondslag voor is, of, in aanvulling, wanneer er toestemming van de betrokkene is. Deze gegevens mogen alleen verwerkt worden met betrekking tot het doel waarvoor ze verkregen zijn. Wij zijn alert op eventuele 'bijvangsten' aan gegevens die onbedoeld/ongewenst tot extra verplichtingen leiden. Dit vraagt om de nodige beheersingsmaatregelen.

Het maximeren van de aandacht op gedrag

- Wij stimuleren actief, bewust verantwoordelijk en alert gedrag, omdat de 'mens' in vele gevallen de zwakste schakel is in het geheel van beheersingsoplossingen;
- Wij zorgen ervoor dat de relevante mensen binnen ons kantoor (zoals de vennoten) op de hoogte zijn van de nieuwe privacyregels en op de hoogte blijven.

Verantwoordelijkheid

De vennoten spelen een cruciale rol bij het uitvoeren van dit informatiebeveiligingsbeleid. Zo is er een inschatting gemaakt van het belang dat de verschillende delen van de informatievoorziening voor ons kantoor hebben, de risico's die ons kantoor hiermee loopt en welke van deze risico's voor ons kantoor onacceptabel hoog zijn. Op basis hiervan hebben de vennoten dit beleid voor informatiebeveiliging opgezet. Zij dragen dit beleid uit naar de organisatie en ondersteunen bij de bewaking en uitvoering ervan.

De vennoten geven een duidelijke richting aan informatiebeveiliging en demonstreren dat zij informatiebeveiliging ondersteunen en zich hierbij betrokken voelen. Dit door het uitbrengen en handhaven van een informatiebeveiligingsbeleid van en voor alle disciplines van het kantoor.

Dit beleid is van toepassing op de gehele organisatie, alle processen, organisatieonderdelen, objecten, informatiesystemen en gegevens(verzamelingen). Het informatiebeveiligingsbeleid is in lijn met het algemene beleid van ons kantoor en de relevante wet- en regelgeving. De vennoten van ons kantoor zijn zelf verantwoordelijk voor het opstellen en/of uitvoeren en/of handhaven van het beleid.

Inwerkingtreding

Dit informatiebeveiligingsbeleid is in werking getreden na vaststelling door de vennoten op 3 mei 2018. Het beleid wordt jaarlijks geëvalueerd en indien nodig herzien.