VGA
LAW & ADR

WHITE PAPER

HET BEROEPSGEHEIM EN GEGEVENSBESCHERMING VOOR ACCOUNTANTS

BELANGRIJKER DAN OOIT

HET BEROEPSGEHEIM ALS VERTROUWENSBRON

Het beroepsgeheim is geen privilege, noch een voorrecht. Het is een last die de gewone discretieplicht overstijgt. Het is een cruciale factor om een omvattende en ethische dienstverlening te kunnen aanbieden.

VEILIG GEDRAG BEGINT BIJ BEWUSTZIJN

Het beroepsgeheim is een breed en abstract begrip voor velen. Welke personen zijn gehouden tot het beroepsgeheim? Welke activiteiten zijn beschermd? Welke elementen en informatie vallen onder het beroepsgeheim?

In deze white paper bieden we een duidelijk overzicht en praktische checklist om het beroepsgeheim te respecteren en uw dienstverlening te optimaliseren.

Het beroepsgeheim en de GDPR-wetgeving

Als advocaat en adviseur van ondernemers zie ik het dag na dag: veel bedrijven investeren in hun dienstverlening, hun klanten en hun groei, maar onderschatten dat gegevens - en de vertrouwelijkheid ervan - een kernonderdeel van de werking zijn. Uw optimale dienstverlening staat of valt met de mogelijkheid om met alle kennis van zaken een professioneel oordeel te vellen.



Om een optimale dienstverlening te garanderen moeten accountants hun opdracht met volledige kennis van zaken kunnen uitvoeren. Uw klant moet er op kunnen vertrouwen dat de vertrouwelijkheid van zijn informatie verzekerd is. Enkel dan zullen ze niet aarzelen om gevoelige - en belangrijke - informatie te delen.

Daarnaast moet uw bedrijf - om het beroepsgeheim te respecteren - de vertrouwelijke gegevens, conform de GDPR-wetgeving, correct verwerken. Datalekken zijn hierbij uit den boze.

Daarom hebben we deze white paper opgesteld. Aan de hand van 7 cruciale punten wordt het beroepsgeheim uiteengezet. Daarna bundelen we inzichten uit de praktijk, wetgeving en concrete tools om bedrijven te helpen hun gegevensbescherming op orde te krijgen. Hiervoor hebben wij een lijst met do's and don'ts ontwikkeld. Zie het als een praktische gids.

Veel leesplezier!

Laura Van Gompel, advocaat-partner

VGA
LAW & ADR

Het beroepsgeheim in 7 punten

Regelgevend kader:

- Wet van 17 maart 2019 betreffende de beroepen accountant en belastingadviseur
- Artikel 458 Strafwetboek
- Institute for Tax Advisors & Consultants

Voor wie?

Het beroepsgeheim is van toepassing op **beroepsbeoefenaars**. Deze term slaat op:

- de (geen) gecertificeerde accountant
- de fiscaal accountant
- de medewerkers en de stagairs die de beroepsactiviteiten uitoefenen als zelfstandige in hoofdberoep of bijberoep, voor rekening van derden.

Welke activiteiten?

Het beroepsgeheim geldt voor alle **professionele activiteiten** die verband houden met de uitoefening van het beroep.

Voor welke informatie?

Alle informatie van vertrouwelijke aard die wordt verkregen in de uitoefening van het beroep. Dit omvat:

- Bedrijfsgevoelige informatie van cliënten en hun medewerkers
- Strategische plannen, commerciële contracten en correspondentie
- Informatie over lopende geschillen, belastingen en onderzoeken
- Elk feit dat de cliënt toevertrouwt, expliciet of impliciet, in de context van de beroepsuitoefening
- Gegevens die niet rechtstreeks worden verkregen door de klant maar via derden (banken, administraties,..)

Ook interne nota's of communicaties met het oog op het uitvoeren van de opdracht, de briefwisseling, de opdrachtbrief van de klant wanneer deze vertrouwelijke informatie bevat en timessheets vallen onder het beroepsgeheim.

Wanneer geldt het beroepsgeheim niet?

Het beroepsgeheim is **niet absoluut.** De wet erkent enkele uitzonderingen:

- Anti-witwaswet
- Verdediging in rechte
- Publieke gegevens

De klant kan de accountant toestemming geven om bepaalde informatie vrij te geven. Als accountant bestaat er desalniettemin een deontologische en contractuele verplichting om deze gegevens niet mee te delen aan derden zonder daartoe het akkoord van de klant of geldige instructie van een autoriteit te ontvangen.

De accountant wordt dus niet ontslaan van het beroepsgeheim wegens het feit dat de klant zijn akkoord zou hebben gegeven om vertrouwelijke informatie openbaar te maken.

De accountant moet, ondanks het akkoord, **zelf beoordelen** of de vertrouwelijkheid die gepaard gaat met de uitvoering van zijn opdracht niet nog steeds geheimhouding vereist.

Waar geldt het beroepsgeheim?

De bescherming van het beroepsgeheim gaat verder dan de stukken die zich bij de accountant bevinden. Ook stukken die zich bij de klant bevinden vallen onder het beroepsgeheim.

Het is dus aangeraden om schriftelijke adviezen aan klanten als **confidentieel** te bestempelen. Zo kan de klant de stukken makkelijker van elkaar onderscheiden wanneer ze worden meegenomen tijdens een controle.

Praktische aanbevelingen

- **Beperk de toegang** tot vertrouwelijke gegevens
- Maak contractuele afspraken voor samenwerkingen met derden
- Creëer bewustzijn bij alle medewerkers
- Ontwikkel interne procedures

Gegevensbescherming in de praktijk

Als accountant bent u constant bezig met gevoelige en vertrouwelijke informatie. Informatie wordt intern gedeeld, uitgestuurd naar de klant, of opgeslagen in het systeem. De bescherming van deze informatie is een belangrijke factor van het beroepsgeheim. Toch vergeten veel bedrijven dat ook data vandaag een kernonderdeel van hun werking zijn. Tot er iets misgaat. We krijgen dan vaak dezelfde reacties: "We hadden niet gedacht dat zoiets ons kon overkomen." Of: "We hadden wel ergens een policy, maar niemand gebruikte ze echt."



Datalekken ontstaan meestal ten gevolge van kleine menselijke fouten: een medewerker die gevoelige informatie naar de verkeerde persoon mailt, een USB-stick of laptop die ergens blijft liggen, een wachtwoord dat hergebruikt wordt of te gemakkelijk te raden is, of toegang tot klantendata die te breed werd gedeeld binnen het bedrijf.

In een accountantskantoor komen daar typische risico's bij: het doorsturen van documenten via onbeveiligde kanalen, verkeerde ingestelde scan-to-mail, automatische doorstuurregels in mailboxen, thuiswerk zonder MDM, of tijdelijke stagairs met blijvende toegangen.

Vaak zijn de gevolgen ingrijpend: een melding bij de Gegevensbeschermingsautoriteit, paniek op de werkvloer, bezorgde klanten, juridische kosten of reputatieschade.

Wat mij telkens opvalt: veel risico's zijn perfect beheersbaar. Met de juiste afspraken, een goede basisopleiding, en een bedrijfscultuur die belang hecht aan dataveiligheid.

VGA
LAW & ADR

Quick wins op de werkvloer? Yes, sir.

Credentials

- Zorg voor een sterk wachtwoord: gebruik minstens 13 tekens of uw vingerafdruk.
- Vermijd het gebruik van voor de hand liggende woorden of zinnen.
- Houd privé en werk gescheiden door verschillende wachtwoorden te gebruiken.
- Verander regelmatig uw wachtwoorden en maak gebruik van een (online) wachtwoordkluis.
- Controleer met regelmaat op gespecialiseerde sites of uw gegevens niet zijn gehackt.



- Voeg een extra beveiligingslaag toe door tweefactorauthenticatie in te stellen.
- Zorg voor een opgeruimde werkomgeving door de clean desk en clean screen methode toe te passen. Laat geen wachtwoorden rondslingeren.



Access

- Deel uw inloggegevens nooit met anderen.
- Gebruik voor andere gebruikers extra autorisatie
- Beperk de toegang tot informatie tot wat strikt noodzakelijk is.
- Sla bestanden niet lokaal op, maar kies voor centrale opslag voor betere beveiliging en automatische back-ups om ongeorganiseerde opslag te voorkomen.
- Laat uw documenten of gegevensdragers nooit onbeheerd achter.
- Laat uw sleutels en toegansbadges niet rondslingeren. rondslingeren.

BYOD & MDM

- Vermijd verwijderbare media zoals USB-sticks, harde schijven.
- Gebruik een heldere mappenstructuur.
- Zorg voor een beveiligde verbinding met werkomgeving vanuit uw thuiscomputer.
- Verstuur geen informatie van uw werk naar uw privé e-mailadres.
- Verbind niet zomaar met openbare wifi zonder VPN.
- Gebruik geen onveilige apps of browsers.
- Bewaar werkdocumenten enkel in bedrijfsomgevingen zoals SharePoint of OneDrive.



Social Media

- Schakel locatievoorzieningen uit en pas tweefactorauthenticatie toe.
- Wees alert bij het downloaden van bestanden of klikken op links.
- Publiceer niet namens uw organisatie zonder toestemming. Deel geen meningen die u of uw organisatie kunnen schaden.
- Deel nooit interne informatie, vertrouwelijke documenten of namen van cliënten of collega's.
- Tag collega's enkel in posts waar zij inhoudelijk bij betrokken zijn én akkoord zijn met de inhoud.



E-mails

- Beperk het verzenden van gevoelige of vertrouwelijke persoonsgegevens.
- Klik niet op verdachte e-mails.
- Schakel het automatisch openen van gedownloade documenten uit.
- Gebruik geen algemene e-mailadressen (zoals info@...) voor persoonlijke opvolging.
- Stuur geen e-mails met een onpersoonlijke of generieke boodschap in BCC naar meerdere ontvangers, tenzij strikt noodzakelijk.
- Gebruik uw inbox niet als archief of takenlijst.
- Behandel binnenkomende e-mails volgens het 4D-principe: Do, Delegate, Defer, Delete.

"Kleine fouten, grote gevolgen? Kleine aanpassingen, grote win."



Gegevensbescherming is vandaag zonder twijfel een zaak voor IT-specialisten, maar eveneens een gedeelde verantwoordelijkheid van elke medewerker, leidinggevende en elk bedrijf.

Met heldere richtlijnen, een gezonde portie bewustzijn en een paar structurele keuzes kunt u als onderneming al heel wat risico's vermijden.

Heeft u vragen over hoe uw organisatie dit concreet kan aanpakken? Wilt u een interne check-up, een duidelijk beleid, of praktische ondersteuning voor uw team?

Wij denken graag met u mee.

TIP: Wist u dat u bij ons team terecht kan voor op maat opleidingen - zowel digitaal als fysiek - voor uw personeel, ICT-partner, management, consultants, etc.?

www.vga.law
info@vga.law
+ 32 1 13 2 8 1 280