**Whitepaper**

# Bescherm jouw accountantskantoor tegen een datalek

Voor accountants- en administratiekantoren

Wolters Kluwer

# Inleiding

Online veiligheid staat in de accountancybranche voorop. Het vertrouwen van klanten is key. In deze whitepaper lees je meer over de **online veiligheid binnen je accountants- of administratiekantoor**. Zo ben je snel op de hoogte van hoe je een datalek herkent en voorkomt. En wanneer je er toch mee te maken krijgt: hoe het beste te handelen en je interne processen hierop in te richten.

# Inhoud


1. **Wat is een datalek?**
   Pagina 4

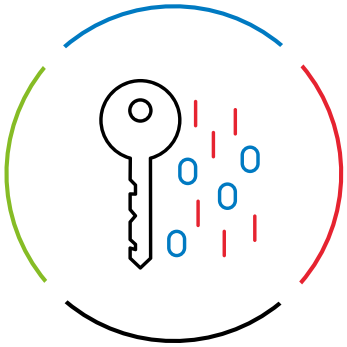
2. **Een datalek voorkomen**
   Pagina 6

3. **Bewustwording creëren**
   Pagina 8

4. **Hackers herkennen**
   Pagina 9

5. **Wat te doen bij een datalek**
   Pagina 10


# 1: Wat is een datalek?



We spreken van een datalek of privacylek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Ook is er sprake van een datalek wanneer persoonsgegevens verloren zijn geraakt en er geen back-up is. Het moet dus gaan om een inbreuk op de beveiliging van persoonsgegevens. De persoonsgegevens zijn niet beschermd geweest, mogelijk verloren of onrechtmatig verwerkt. Een voorbeeld van een datalek is het kwijtraken van een USB-stick met daarop persoonsgegevens.

### Enkele voorbeelden van datalekken:

- Een e-mail wordt verzonden waarin de e-mailadressen van alle geadresseerden zichtbaar zijn voor alle andere geadresseerden (in CC in plaats van BCC).
- Een online dienst of databestand wordt gehackt, waardoor klantgegevens gestolen konden worden.
- Een DDOS-aanval leidt ertoe dat een ziekenhuis gedurende 30 uur medische dossiers niet in kan zien.
- Persoonsgegevens van een groot aantal studenten worden naar de verkeerde mailinglijst verzonden.
- Een USB-stick met persoonsgegevens is kwijtgeraakt of een laptop is gestolen.

Wanneer hackers het netwerk van jouw kantoor binnendringen of doordat je bijvoorbeeld jouw laptop in de trein laat liggen en je daardoor data verliest, spreken we niet direct van een datalek. Je hoeft hiervan nog geen melding te maken bij de Autoriteit Persoonsgegevens.

Registreer een dergelijk voorval wel altijd intern en pas je procedures hierop aan. We spreken van een datalek wanneer de gegevens van de personen die gelekt zijn gevoelig zijn en de hackers op basis hiervan de rechten en vrijheden van deze personen kunnen schenden. Gaat het bijvoorbeeld om losse e-mailadressen, dan hoef je je niet direct zorgen te maken, maar wanneer de boekhouding van een klant op straat ligt, moet je direct actie ondernemen.

## Meestal menselijke fout

De meeste datalekken worden in de praktijk veroorzaakt door menselijke fouten. Ongelukjes en slordigheden die ontstaan door een hoge werkdruk waarbij zelden opzet in het spel is. Drie veel voorkomende oorzaken zijn:

1 E-mail met persoonsgegevens verstuurd aan de verkeerde persoon
2 Klikken op link of bijlage openen van phishing e-mail
3 Verloren telefoon

'Dat er data onbedoeld wordt gelekt is bijna aan de orde van de dag. Het Donorregister, ziekenhuizen... Ik noem een paar recente voorbeelden. Zeker als dienstverlener waar je met gevoelige data van klanten werkt zoals accountants, is het voorkomen van schade door datalekken heel belangrijk.

Toch kun je datalekken zelf bijna niet voorkomen. Ik vergelijk het wel eens met een huis. Je kunt het nog zo goed beveiligen, maar als dieven binnen willen komen, lukt dat ze helaas toch wel. De mens is de zwakste schakel. De achterdeur van je huis open laten staan, een mail met alle geadresseerden in de cc in plaats van de bcc, memorysticks die uitgedeeld worden met malware, een verkeerde klik op een mail...'

**Menno Weij**,
Partner Tech & Privacy Law BDO

# 2: Een datalek voorkomen

Om een datalek te voorkomen, is het essentieel de juiste voorzorgsmaatregelen te treffen en processen in plaats te hebben. De volgende stappen kunnen hierbij helpen:

1 **Wijs een functionaris voor de gegevensbescherming aan**

Een ‘functionaris gegevensbescherming’ is verantwoordelijk voor het beleid op het beschermen van persoonsgegevens. Meestal is dit de compliance officer binnen de organisatie. Deze moet toezicht houden en controleren of medewerkers het beleid nastreven. Voor publieke organisaties is het aanstellen van een compliance officer zelfs verplicht.

2 **Breng gegevensstromen in kaart**

Zorg ervoor dat je zicht hebt op welke personen binnen jouw organisatie toegang hebben tot kwetsbare persoonsgegeven en hoe ze dit verwerken. Zo kan een datalek eenvoudiger te traceren zijn. Heb je geen paperless office? Dan geldt dit ook voor hardcopy documenten.

### 3 Maak gebruik van encryptie

Versleutel gevoelige informatie die je per e-mail verstuurd. Versleutelde berichten kunnen namelijk alleen gelezen worden door mensen die de sleutel hebben. Zo voorkom je dat deze informatie in verkeerde handen terecht komt.

### 4 Wees kritisch op wat je bewaart

Je kunt het beste gegevens verwijderen met een verstreken bewaartermijn en die niet van nut zijn voor de organisatie.

### 5 Zorg voor goede beveiliging

Maak gebruik van een goede virusscanner en firewall voor het beschermen van jouw gegevens. Zorg voor een beleid op wachtwoorden en hou je software up te date. Dit geldt ook voor je website.

### 6 Leg een protocol vast

Leg vast in een protocol wie er gebeld moet worden als het misgaat. En wat er vervolgens allemaal moet worden gedaan om schade te beperken. Dat geldt ook voor de kleine accountant! Weet ook wie je moet hebben bij je externe leveranciers. Houd iedereen scherp en trek lessen uit wat er is gebeurd. Processen zijn niet in beton gegoten! Ze moeten periodiek geupdate worden. Zorg voor een beleid op wachtwoorden en hou je software up te date. Dit geldt ook voor je website.

'Het belangrijkste is dat je iemand aanstelt die alles ter plekke kan afhandelen en weet bij wie hij zich moet melden. Het beste is dat sowieso in ieder bedrijf te regelen. Wat ook heel belangrijk is, is dat iedereen in de organisatie weet wat een datalek is. Slim is om bijvoorbeeld een e-mailadres aan te maken waar iedereen met vragen terecht kan. Bijvoorbeeld: privacy@naambedrijf.nl. Daarmee verlaag je een grens en zullen mensen ook kleinere incidenten voor de zekerheid doorsturen.'

**Richard Ridderhof,**
Compliance Officer Twinfield

'In bedrijven test je eens in de zoveel tijd het brandalarm. Via een protocol volg je de stappen die je moet doen. Ook een datalek is een incident dat je dus moet beschrijven in een protocol. Beschrijf stap voor stap wat mensen moeten doen als privacy-gevoelige gegevens onbedoeld op straat komen, en wie het aanspreekpunt is. Herhaal en test het net als bij een brand-alarm of reanimatiecursus bijvoorbeeld vier keer per jaar. Door de kracht van herhaling creëer je instinct en weten mensen wat ze moeten en kunnen doen. Dan raken ze niet in paniek en zijn ze niet bang om iets te melden.' - **Menno Weij**

'De basis hygiëneregels moeten bij iedereen duidelijk zijn. Bijvoorbeeld nooit privacygevoelige gegevens op een memorystick, sluit een computer af wanneer je niet meer achter een bureau zit, laat laptop niet in auto achter. Dit zijn kleine basistips die de kans op datalekken verkleinen.'

**Menno Weij**,
Partner Tech & Privacy Law BDO

# 3: Bewustwording creëren

Wanneer persoonsgegevens door een fout op straat komen te liggen, is de organisatie die de fout gemaakt heeft aansprakelijk voor de schade die daaruit voortvloeit. Deze schade kan miljoenen kosten. Denk aan materiele schade (boetes, claims van betrokkenen) en immateriële schade zoals imag0schade of psychische schade voor betrokkenen. Bij overtreding van de meldplicht kan een boete van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet opgelegd worden. Bewustwording van alle medewerkers is daarom essentieel om grote schade te voorkomen.
Deze 4 stappen helpen hierbij:

1 **Leg de risico's uit**

Leg aan iedereen in het bedrijf uit wat de risico's zijn. Naast de boetes staat ook reputatie van je bedrijf op het spel. Denk bij het creëren van die bewustwording aan het fenomeen 'Vreemde ogen dwingen'. Huur een expert in, de informatie komt dan anders binnen bij je medewerkers.

2 **Herhaal de boodschap**

Leg de risico's niet één keer uit, maar zorg voor meerdere momenten van bewustwording.

3 **Neem angst weg**

Zorg ervoor dat werknemers die de oorzaak zijn, niet weg willen kruipen onder een bureau. Zorg dat ze wel onmiddellijk in actie komen om meer ellende te voorkomen. 'Wees niet bang om te melden' moet de boodschap zijn voor iedereen.

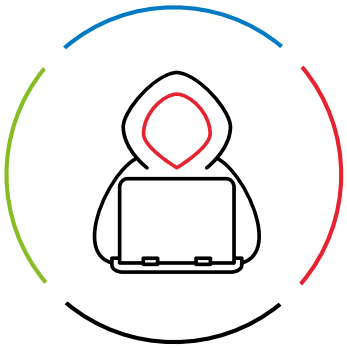
4 **Zorg voor duidelijke 'hygiëneregels'**

De basis hygiëneregels moeten bij iedereen duidelijk zijn. Bijvoorbeeld nooit privacygevoelige gegevens op een memorystick, sluit een computer af wanneer je niet meer achter een bureau zit, laat laptop niet in auto achter. Dit zijn kleine basistips die de kans op datalekken verkleinen.

'Openheid en eerlijkheid is echt heel belangrijk om schade te voorkomen. Zorg dus voor een open bedrijfscultuur in je bedrijf. Zodat zaken niet onder de pet blijven en mensen durven te melden. Train personeel over datalekken en zorg bijvoorbeeld voor een bewustzijnstraining.'

**Richard Ridderhof,**
Compliance Officer Twinfield

# 4: Hackers herkennen



Het aantal datalekken door hacking of phishing is helaas sterk groeiende. Een hacker stuurt vaak berichten die een beroep doen op onze kwetsbaarheden, inhaken op nieuws van de dag of een andere urgentie. In onze haast of nieuwsgierigheid klikken we op de link en het kwaad is geschied. Het is dus van belang om altijd de volgende zaken in acht te nemen bij e-mails:

## Check de betrouwbaarheid van de afzender:

- Controleer het e-mailadres. Vaak is het e-mailadres een afgeleide versie van de echte bedrijfsnaam. Emailadressen met vreemde namen en/of cijfers zijn verdacht.
- Check altijd de link die genoemd wordt in de e-mail. Dit doe je door er met je muis overheen te gaan. Het betreffende website adres (url) zie je dan onder de muisknop. Komt het wel overeen met de echte site?
- Kijk goed naar onregelmatigheden. Kon je vroeger een nepmail makkelijk herkennen aan het slechte taalgebruik, vandaag de dag gebruiken hackers correcte logo's en betere spelling.

## Wees kritisch op de inhoud van e-mails:

- De meeste bedrijven waar je zaken mee doet hebben jouw persoonsgegevens en zullen die ook gebruiken in de aanhef.
- Ontvang je een bericht met de vraag om persoonsgegevens aan te vullen door op een link te klikken? Doe dit niet! Banken, verzekeraars en overheidsinstanties zullen dit nooit op deze manier doen.
- Hackers spelen in op urgentie. Ze proberen je in te laten spelen op zaken als. 'Uw hosting-pakket verloopt, maak € 150,- over via onderstaande link wanneer u uw gegevens niet kwijt wilt raken'. Wanneer je twijfelt, kun je het beste contact opnemen met jouw eigen hostingpartij.
- Open nooit zomaar een bijlage van een onbekende afzender. Virussen of malware kunnen makkelijk verstopt worden in een bijlage. Bij twijfel kun je het beste contact opnemen met jouw IT-afdeling of de mail verwijderen.

## Gehackt?

Denk je dat je gehackt bent?
Neem dan de volgende acties:

- Verander je wachtwoord. Je kunt hiervoor ook een vertrouwde wachtwoord manager gebruiken die je versleutelt met een master-key. Bij twijfel kun je altijd jouw IT-afdeling raadplegen welke wachtwoordmanager betrouwbaar is.
- Controleer je instellingen en gegevens.
- Breng betrokkenen op de hoogte.
- Neem contact op met IT.
- Neem contact op met je provider.
- Controleer je PC op virussen en/of malware.


Cybercriminaliteit komt steeds vaker voor. Hoe bescherm je je optimaal tegen deze risico's en vergroot je je online veiligheid? De checklist 'Veilig omgaan met persoonlijke data' helpt jou en je collega's veilig om te gaan met (gevoelige) gegevens! Download gratis!

# 5: Wat te doen bij een datalek

Natuurlijk doe je er als bedrijf alles aan om lekken van privacy gevoelige data te voorkomen. Maar wat als er nu toch data lekt? Dan is het zaak om snel inactie te te komen en de volgende stappen te nemen:

1. **Vaststellen of het gaat om een datalek**
2. **Informatie verzamelen**
3. **Een actief datalek stoppen**
4. **Het datalek melden**
5. **Betrokkenen informeren**
6. **Schade beperken**
7. **Een datalek in de toekomst voorkomen**


Deze stappen staan beschreven in het Stappenplan: Wat te doen bij een datalek. Ook dit stappenplan kun je gratis downloaden.

## Deze whitepaper wordt je aangeboden door Twinfield

Twinfield Boekhouden is een professioneel en compleet online boekhoud-programma, waarmee je slim en gemakkelijk online samenwerkt met je accountant. Twinfield Boekhouden koppelt met bijna alle webwinkelsoftware. Zo worden je verkopen eenvoudig geregistreerd en heb je actueel inzicht in de resultaten. Je gegevens zijn zeer veilig en je werkt volledig in de cloud. Twinfield Boekhouden werkt ook goed bij grote aantallen transacties en helpt je bij foutloze btw-aangiftes.

## Over Wolters Kluwer

Wolters Kluwer is een van de grootste aanbieders van informatie, software, tools en diensten voor juridische en fiscale professionals. Wereldwijd werken honderd-duizenden van hen elke dag met onze software. Voor hun dagelijks werk vertrouwen zij op onze jarenlange expertise en op onze producten. De divisie Tax & Accounting levert professionele software, waaronder Twinfield Boekhouden, Twinfield Samen-werken, Alure Online, Basecone en Avanzer Aangifte.

## Contact

Twinfield | De Beek 9-15
3871 MS | Hoevelaken | The Netherlands
www.twinfield.nl | +31 (033) 467 70 10