# HOFFMANN TIPS

voor bedrijfsleven en publieke sector

## Casus: Onverklaarbare verschillen

## Casus: Een oude bekende

## Red Teaming: denken als de vijand

## Datavalidatie, een innovatieve toevoeging bij screening

## Informatiebeveiliging bij Holland Casino

**Interview met Janny Wierda over het cruciale gedrag van medewerkers**

## Mag iedere ziekenhuis-medewerker het patiëntendossier van Barbie inzien?

## Risicomanagement in 7 stappen

**Fred Teeven over het in kaart brengen en analyseren van risico's**

#235
Juli 2018

COLUMN

# D-day 25 mei 2018

**25 mei 2018 is een datum die de gemoederen de afgelopen maanden flink heeft beziggehouden. Zo heeft u ook vast heel wat mails over nieuwe toestemming in uw inbox gekregen. Ook voor ons was 25 mei een harde deadline. We wilden de puntjes op de i zetten, zodat we volgens de nieuwe privacyverordening kunnen werken. En dat is gelukt. Ook in deze Tips komt u verhalen over privacy en informatieveiligheid tegen. En nog veel meer …**

**Cyberveiligheid bij onze klanten**
Naast onze interne werk aan cyberveiligheid helpen we ook onze klanten met het cyberveilig maken van hun organisatie. In deze Tips besteden we aandacht aan Holland Casino die met de hulp van onze sociaalpsychologen een heel programma op gebied van cyberveilig gedrag uitvoerde. Pas als je de redenen voor gedrag van mensen onderzocht hebt, kun je namelijk de juiste maatregelen nemen.

**Meten is weten …**
Maar welke maatregelen zijn nodig? In deze Tips aandacht voor Red Teaming, een dienst waarbij we uw organisatie binnen proberen te dringen, zowel fysiek als digitaal, om te testen hoe goed uw beveiliging werkt. Een gesimuleerde aanval die veel inzicht geeft.

**Hoffmann is en blijft recherche**
Ook in 2018 is de vraag naar ‘wie heeft dit gedaan?’ en ‘hoe heeft het plaats kunnen vinden?’ zeer actueel. Dagelijks benaderen bedrijven en organisaties ons, omdat ze onverwacht worden geconfronteerd met fraude of ander onrechtmatig handelen. Ons handelsmerk van onze manier van werken is snel, discreet en gedegen. Hoffmann blijft de ervaringen uit de alledaagse rechercheprakijk met u delen. Ook in deze Tips.

**Een bijdrage van onze partners**
Zowel Lexence advocaten (arbeidsrecht) als Capra advocaten (ambtenarenrecht) leveren een bijdrage aan deze Tips. Juist deze samenwerking met gerenommeerde advocatenkantoren biedt Hoffmann de gelegenheid haar kwaliteit te verbeteren. Want feedback is hiermee verzekerd!

Een Tips vol met casussen en interessante onderwerpen dus. Ik wens u veel leesplezier!

*Martijn van de Beek*

CASUS

# Onverklaarbare verschillen

**Diefstal van brandstof aan de benzinepomp door weg te rijden zonder te betalen komt in Nederland helaas nog veelvuldig voor. Maar de volgende casus is redelijk uniek. Deze casus speelde bij een leverancier van brandstof aan tankstations. Hij benaderde ons, omdat hij te maken had met onverklaarbare verschillen in het aantal liters brandstof dat werkelijk werd geleverd en het aantal dat in de administratie van de chauffeur stond. Tijd voor actie dus. In overleg met de opdrachtgever werd besloten om observaties uit te gaan voeren.**

### Observeren: een kwestie van lange adem

De eerste week van observatie? Die gaat voorbij zonder resultaat. In de vroege ochtenduren volgen we de vrachtwagen met brandstof. Maar we constateren niets bijzonders. In de tweede week van observaties is het raak. De chauffeur moet aan het einde van de dag nog één tankstation bevoorraden. Bij het tankstation zet hij de vrachtwagen op de juiste plaats en begint hij met het lossen. Het tankstation sluit, maar het lossen gaat nog even door. Na enige tijd komt er een zwarte bestelbus aangereden. Onze medewerkers zien dat er een slang vanaf de vrachtwagen naar de bestelbus gaat.

### In de achtervolging

Na een tijdje vertrekt de zwarte bestelbus. Onze medewerkers besluiten om de bestelbus te volgen. Daarbij zien ze dat de bestelbus wel erg diep in de veren hangt. Ook ruiken ze een enorme brandstoflucht. Dat is dus vast een verklaring voor de verschillen tussen werkelijke liters en liters in de administratie. Toch besluiten ze om de bestelbus niet al te lang te volgen. Ze willen namelijk niet opvallen en zo verdere plannen verstoren. Ze nemen direct contact op met de opdrachtgever en maken een plan voor de volgende dag.

### Nog verder afwachten?

De volgende dag wordt in overleg met de opdrachtgever besloten om gelijk in actie te komen. Onze observanten zien namelijk dat de zwarte bestelbus direct achter de vrachtwagen een terrein op rijdt. Onze medewerkers bellen direct de politie. Die is snel ter plaatse en kan de chauffeur en de twee mannen in de bestelbus aanhouden. Op heterdaad betrapt! In de zwarte bestelbus staan twee tanks van 1.000 liter… Later blijkt dat de uiteindelijke schade voor onze opdrachtgever enorm is. De chauffeur blijkt tienduizenden liters brandstof ontvreemd te hebben.

BIJDRAGE DOOR FRANK TER HUURNE VAN ONZE NETWERKPARTNER LEXENCE

# Ontslag wegens fraude is geen ABC'tje

**Elk jaar worden duizenden Nederlandse bedrijven getroffen door fraude. In bijna driekwart van de gevallen wordt die fraude gepleegd door medewerkers. Daarmee is fraude een belangrijke grond van ontslagprocedures. Maar, ontslag wegens fraude houdt niet automatisch stand. Er kunnen allerlei problemen ontstaan in de procedure. In dit artikel behandelt Frank ter Huurne, advocaat/partner arbeidsrecht bij Lexence, een aantal aandachtspunten.**

### 1. Een zorgvuldig onderzoek

Vermoedt u als werkgever dat een medewerker zich schuldig maakt aan fraude? Dan wilt u dat natuurlijk onderzoeken. Dat kunt u op verschillende manieren doen: een eigen intern onderzoek, een onderzoek door een recherchebureau of forensisch accountant of een justitieel onderzoek. Het belangrijkste nadeel van een intern onderzoek is dat dit meestal niet als onafhankelijk wordt beschouwd. Een onderzoek door een recherchebureau of forensisch accountant is onafhankelijker. Toch blijft u als werkgever verantwoordelijk, ook als u het onderzoek uitbesteedt. Onzorgvuldig onderzoek door een externe partij leidt in ontslagprocedures namelijk vaak tot vervelende complicaties voor u als werkgever.

### 2. Een proportioneel onderzoek

De rechter toetst of het onderzoek van de werkgever aan de wettelijke kaders voldoet. Zoals bijvoorbeeld aan artikel 7:611 BW (goed werkgeverschap), artikel 10 van de Grondwet (recht op privacy) en de AVG. Vanzelfsprekend moet er een concreet vermoeden van fraude bestaan voordat de werkgever overgaat tot onderzoek. De werkgever mag echter niet zomaar een recherchebureau hiervoor inschakelen zonder dat de medewerker dit weet. Dat mag alleen in zeer bijzondere omstandigheden: als er ernstige verdenkingen zijn en een onderzoek buiten de medewerker om noodzakelijk is. Ook moet een werkgever rekening houden met de inbreuk van het onderzoek. De inbreuk op de belangen van de medewerker mag niet onevenredig zijn in verhouding tot het doel van het onderzoek (proportionaliteit). Daarbij moet de werkgever ook beargumenteren waarom het doel niet op een minder ingrijpende manier kan worden verwezenlijkt (subsidiariteit).

### 3. Schorsing tijdens het onderzoek

Het kan noodzakelijk zijn om een betrokken medewerker te schorsen als het onderzoek begint. Daarbij is het wel belangrijk dat de werkgever er van uitgaat dat de betrokken medewerker onschuldig is zo lang de fraude nog niet is bewezen. Dit noemen we de 'onschuldpresumptie'. De werkgever mag de medewerker dus niet op de één of andere manier als schuldige behandelen. Voor een schorsing moet er een gegronde reden zijn. Is die er niet? Dan moet de medewerker gewoon worden toegelaten tot het werk.

Lexence
advocaten & notarissen

### 4. Hoor en wederhoor

Een werkgever moet het beginsel van hoor en wederhoor toepassen. Tijdens een onderzoek moet de werkgever zich namelijk als een goed werkgever gedragen (artikel 7:611 BW). We kunnen op basis van de rechtspraak concluderen dat de werkgever de medewerker niet altijd hoeft te horen bij een voorgenomen ontslag. Toch raad ik u aan om een medewerker wel altijd te horen. Dit voorkomt namelijk dat u met een eenzijdige blik naar de situatie kijkt ('tunnelvisie') en dat u daardoor te snel een ontslag op staande voet kunt geven.

### 5. Eisen bij ontslag op staande voet

Blijkt de medewerker zich schuldig te hebben gemaakt aan fraude? Dan kan de werkgever de medewerker op staande voet ontslaan. De wet stelt drie eisen aan een rechtsgeldig ontslag op staande voet:

1. Er moet sprake zijn van een dringende reden.
2. De werkgever moet de werknemer onverwijld hebben ontslagen.
3. De werkgever moet de dringende reden onverwijld hebben meegedeeld.

U voldoet trouwens ook aan de eis van onverwijld ontslaan als u het recht van hoor en wederhoor toepast of eerst nog (juridisch) advies inwint. Volgens de Hoge Raad vergt zorgvuldig onderzoek nu eenmaal tijd. Maar zodra is vastgesteld dat de medewerker zich schuldig heeft gemaakt aan fraude, moet u als werkgever voortvarend handelen. U kunt de medewerker bijvoorbeeld niet nog een paar dagen laten doorwerken.

### Geen ABC'tje dus

Bij ontslag wegens fraude zijn voorzichtigheid en tegelijk voortvarend handelen geboden. Voor het instellen van een onderzoek door een recherchebureau of forensisch accountant is een concrete verdenking vereist en een onderzoek mag niet lichtvaardig worden ingesteld. Dit geldt ook voor schorsingen gedurende het onderzoek: ook deze maatregel moet noodzakelijk zijn en vergt een deugdelijke motivering. En het beginsel van hoor en wederhoor moet altijd worden toegepast. *Better safe than sorry.*

CASUS

# Dan zoeken we het toch gewoon hogerop …?

**Onze opdrachtgever die milieu gerelateerde werkzaamheden verricht, moet bewijs verzamelen voor de rechtszaak die hij heeft aangespannen tegen een concurrent. Deze concurrent heeft een zakelijk alleenrecht verworven dat een groot gebied bestrijkt. Gezien het enorme prijsverschil waardoor de concurrent gewonnen heeft moet volgens de opdrachtgever de concurrent wel milieudelicten plegen en zich niet aan de strenge regels houden. Er zijn gewoonweg veel kosten mee gemoeid om volgens de regels te kunnen werken. Maar ja, dat moet de opdrachtgever natuurlijk wel kunnen bewijzen. Pas dan kan hij aantonen dat er sprake is van oneerlijke concurrentie. Hij verliest momenteel nog meer klanten doordat hij zich wel aan de regels houdt en de concurrent niet. Hij is daardoor namelijk duurder en minder slagvaardig. Deze oneerlijke concurrentie zou hem tonnen schade opleveren.**

### Observeren en volgen

We kunnen eventuele milieudelicten alleen vaststellen door te observeren en te volgen. In de praktijk blijkt dit alleen vrijwel onmogelijk. Juist door de milieucomponent lukt het in bijna geen enkel geval om bij de te observeren bron te komen. De omgeving die we observeren is divers: stedelijk gebied, landelijk gebied en waterrijk gebied. Helaas is er simpelweg geen of zeer beperkt zicht. We proberen nog om vanuit hoger gelegen locaties te observeren en feiten vast te leggen. Maar het leidt helaas tot niets.

### Een nieuw plan

Eén van onze observanten komt met het idee om een helikopter in te zetten. Iets wat we nog niet eerder hebben toegepast binnen Hoffmann. Het is een oplossing om toch goed te kunnen observeren en eventuele milieudelicten te kunnen vastleggen. De opdrachtgever is enthousiast! We schakelen een bedrijf in voor de helivluchten. Eén van onze observanten vliegt mee en kan veel foto's maken. We voeren meerdere vluchten uit: op verschillende dagen, op verschillende tijden en tijdens een langere periode. Zo kunnen we structurele overtredingen vaststellen en gaat het niet om momentopnames. De resultaten zijn verbluffend goed. De vermoedens van onze opdrachtgever kloppen. Het observatierapport met fotobijlage heeft hij tijdens de rechtszaak kunnen gebruiken.

### Van het een komt het ander ...

Na afloop evalueren wij intern de inzet van de heli. We komen tot de conclusie dat luchtondersteuning vaker wenselijk is om adequaat te kunnen observeren. De inzet van een heli kost veel geld maar gelukkig zijn er tegenwoordig betaalbare oplossingen beschikbaar. Hoffmann heeft daarna enkele drones gekocht en er zijn inmiddels drie observatiemedewerkers van Hoffmann opgeleid tot volwaardig dronepiloot. Ook is Hoffmann vergunninghouder voor beroepsmatig vliegen met drones. Bij eventuele beperkingen kunnen we alsnog een heli inzetten. Beide middelen helpen ons bewijslast te verzamelen waar dat op een andere manier niet mogelijk is.

CASUS

# Een oude bekende

**Regelmatig voeren we onderzoeken in de zorg uit. Vaak omdat er geld wordt gestolen van cliënten. Zo ook een aantal jaar geleden. We deden onderzoek bij een zorginstelling voor geestelijk gehandicapten. Uiteraard zijn onze medewerkers altijd vastberaden om de fraude op te lossen, maar dit geldt zeker wanneer de slachtoffers uit een kwetsbare doelgroep komen. In overleg met de klant plaatsten we een geheime camera. Al snel bleek dat een verzorger tijdens de nachtdienst geld uit kastjes van cliënten wegnam. Onze medewerkers confronteerden de jongeman en na een volledige bekentenis zat zijn dienstverband bij de zorginstelling erop.**

### Een andere zorginstelling, dezelfde vraag

Onlangs meldt zich een andere zorginstelling in dezelfde regio bij Hoffmann voor een onderzoek. Geen bijzonderheid, want in de zorg voeren we regelmatig onderzoeken uit. Ook bij deze zorginstelling wordt geld gestolen van cliënten. In dit geval zijn de cliënten ouderen die niet meer zelfstandig kunnen wonen. Ook bij deze zorginstelling hebben we in overleg met de klant een geheime camera geplaatst. De opdrachtgever neemt niet veel later contact met ons op: er staat iemand op beeld. Helaas staat niet de diefstal op beeld, maar een medewerker die porno kijkt op een computer van een cliënt en hierbij ook seksuele handelingen bij zichzelf verricht.

### Gesprek met een oude bekende?

We hadden de geheime camera met een ander onderzoeksdoel ingezet. De vraag is: wat nu? We maken de afweging om toch een gesprek met de betreffende medewerker te voeren. Als de medewerker de gespreksruimte binnenkomt, merkt één van ons op dat hij 'een bekend gezicht' heeft. De medewerker geeft aan nooit eerder met iemand van Hoffmann te hebben gesproken. Tijdens het gesprek schiet het onze medewerker ineens te binnen: hij kent deze jongeman van het onderzoek een paar jaar eerder! Dat blijkt uiteindelijk te kloppen. Ook bekent hij seksuele handelingen bij zichzelf te hebben verricht achter de computer van een cliënt. Maar volgens hem heeft hij niets te maken met de diefstal van geld.

### Probleem opgelost

Onze opdrachtgever ontslaat de jongeman op staande voet vanwege zijn gedrag. Een paar weken later informeren wij bij de opdrachtgever of er nog diefstallen zijn geweest. 'Niet meer na het vertrek van de jongeman …' Onze oude bekende was waarschijnlijk toch in het oude diefstalgedrag teruggevallen. Een casus die tevens aantoont dat een goede personeelsscreening ook van groot belang is!

# Red Teaming: denken als de vijand

**“De digitale weerbaarheid van Nederland loopt achter op de groeiende dreiging. We worden geconfronteerd met uiteenlopende vormen van digitale aanvallen gericht op politieke en economische spionage en cybercriminaliteit.”**

Een uitspraak van de minister van Buitenlandse Zaken Stef Blok in april. Het ministerie waarschuwde leden van de handelsmissie naar China voor spionage. Allerlei voorzorgsmaatregelen waren het gevolg: nieuwe telefoons zonder onnodige apps en met extra beveiliging, belangrijke documenten gingen alleen geprint mee en laptops kregen geüpdate beveiligingssoftware.

### Hoe zeker bent u over uw digitale weerbaarheid in Nederland?

Niet alleen bij handelsmissies in andere landen ligt het gevaar op de loer. In de afgelopen jaren is het lekken van belangrijke, gevoelige informatie regelmatig in het nieuws. De cijfers liegen er niet om: het duurt gemiddeld 252 dagen voordat een bedrijf erachter komt gehackt te zijn, terwijl in 82% van de gevallen de hack zelf binnen één minuut gebeurd is. Mensen die kwaad willen, houden zich niet aan regels en procedures. Ze maken gebruik van de kwetsbaarheid en hulpvaardigheid van de mens of van zwakheden binnen uw IT-systeem. Dat maakt het ingewikkeld om het aan het licht te krijgen.

*Ons team van ethical hackers, voice-phising-specialisten en fysieke-inloop-specialisten wist uiteindelijk toegang te krijgen tot kritieke informatiesystemen.*

### Red Teaming brengt onzichtbare dreigingen aan het licht

Wacht niet af, maar neem zelf het heft in handen. Red Teaming kan u daarbij helpen. Het is een methode die uit het leger komt. Militaire eenheden testen elkaar daarbij op hun defensieve capaciteit. Concreet valt het ‘Red team’ het ‘Blue team’ aan. De kracht van Red Teaming is: denken als de vijand, out-of-the-box in plaats van de geijkte tactieken. Een mooi voorbeeld is de Red Teamingstest van admiraal Harry E. Yarnell in 1932. Op een vroege zondagmorgen viel hij de schepen in Pearl Harbor aan met een precisie-luchtaanval: er vielen zakken meel op de schepen in de haven. Daarmee toonde hij aan dat Pearl Harbor kwetsbaar was voor een luchtaanval op zee. Helaas vond het ministerie van Defensie dat een dergelijke aanval geen realistisch scenario was. We weten allemaal hoe dat bijna tien jaar later afliep.

### Red Teaming in de praktijk

Een opdrachtgever vroeg zich af of het mogelijk was om van binnenuit een aanval te lanceren op het netwerk. Iemand kan bij deze organisatie alleen binnenkomen via een 1-persoonstourniquet. Daarvoor moet je je eerst melden bij de portier die je ID controleert. Wij voerden een Red Teaming test uit voor deze opdrachtgever. En met succes. Ons team van ethical hackers, voice-phising-specialisten en fysieke-inloop-specialisten wist uiteindelijk toegang te krijgen tot kritieke informatiesystemen. Zo kon het team zwakheden blootleggen en deze delen met de opdrachtgever.

### Hoe gingen we te werk?

Onze specialisten begonnen met een voice-phising-actie: ze belden medewerkers van de klant met een smoes. Op deze manier wisten ze wachtwoorden te ontfutselen. Vervolgens maakten onze inloopspecialisten na een gedegen voorverkenning een plan om het gebouw binnen te dringen. Twee specialisten wisten na een geslaagde afleidingsmanoeuvre binnen te komen. Eenmaal binnen gingen zij op zoek naar een flexplek waar zij een connectie konden maken met het netwerk. Dit kostte even wat meer tijd, aangezien een aantal netwerkpoorten blijkbaar goed afgeschermd waren. Uiteindelijk vonden ze een geschikte poort in een afgelegen printerruimte. Daar konden ze de meegebrachte, geprepareerde laptop op aan sluiten. De ene collega hield de wacht, de andere voerde een scan en aanval uit op het netwerk. Al snel konden we aantonen dat we op deze manier toegang konden krijgen tot kritieke informatie van de opdrachtgever. Uiteraard hield daar de test op en hebben we de klant over de kwetsbaarheden geïnformeerd.

### Het resultaat van Red Teaming

De resultaten van onze aanval gaven inzicht aan de opdrachtgever. Het gaf hem de mogelijkheid om aanvullende maatregelen te nemen om de kwetsbaarheden te beheersen. De wachtwoorden hebben we uiteindelijk niet gebruikt, maar het gaf wel aan dat de opdrachtgever aandacht moest geven aan het security bewustzijn van zijn medewerkers.

COLUMN

# De menskant van informatiebeveiliging bij Holland Casino

Veilig gedrag treedt op als iemand het wil doen (motivatie), het kan doen (capaciteit) en in staat wordt gesteld om het te doen (gelegenheid). Het Hoffmann 3x3-model helpt organisaties om grip te krijgen op gedrag. Eerst bekijken onze sociaalpsychologen waarom bepaald gewenst gedrag nu nog niet optreedt. Vervolgens kijken we welke menselijke, technische en organisatorische stappen er bij een gewenste gedraging te nemen zijn. Bewustwording is daar slechts een onderdeel van.

**KLANT AAN HET WOORD**

### “Het gedrag van medewerkers is cruciaal”

“Informatieveiligheid is voor Holland Casino een van de pijlers onder ons programma ‘Veilig en verantwoord spel’, naast ons Preventiebeleid voor kansspelen en de verplichtingen die wij hebben rondom geldstromen (Wwft). Ons eerste verzoek aan Hoffmann was een scan van onze informatiebeveiliging. Hoffmann heeft vervolgens de aanbeveling gedaan om de menselijke kant van informatieveiligheid te versterken. Het gedrag van medewerkers is cruciaal als het gaat om informatiebeveiliging. In ons bedrijf staan gasten centraal en behalve een betrouwbaar spel willen we ook hun privacy waarborgen. Samen met Hoffmann zijn we begonnen aan een programma om informatieveilig gedrag op kantoor en in de casino’s te stimuleren, wat veel verder gaat dan ‘awareness’ en verder dan alleen maar kennis delen met de medewerkers. Door de gerichte aanpak die Hoffmann hierin heeft gebracht, kunnen we medewerkers ondersteunen in hun dagelijkse werk. Zo leveren we een positieve bijdrage aan hun werk en aan onze informatieveiligheid. Door de gerichte aanpak en ondersteuning op juist die plekken waar dat nodig is, kreeg het programma al snel draagvlak in de hele organisatie. Op deze manier kunnen we informatieveiligheid in ons bedrijf borgen en onze reputatie als betrouwbaar casino waarmaken.”

*Janny Wierda*
*directeur Security & Responsible Gaming*

# Datavalidatie, een innovatieve toevoeging bij screening

Steeds meer bedrijven kiezen ervoor om sollicitanten en medewerkers te screenen. Niet alleen als dat verplicht is volgens wet- en regelgeving. Hoffmann biedt op het gebied van screening verschillende vormen van dienstverlening. Niet alleen screening, maar ook datavalidatie. Datavalidatie betekent dat we de data in bijvoorbeeld het CV controleren op onwaarheden. Ook het aanvragen van een VOG kan hier onderdeel van zijn. Wij voeren datavalidatie uit in samenwerking met onze partner Validata Group.

### Noodzaak van datavalidatie

Bij screening houden we altijd een persoonlijk interview met een potentiële kandidaat en doen we een uitgebreide referentencheck. Zo brengen we mogelijke risico’s voor de opdrachtgever in beeld. Datavalidatie is daarbij een waardevolle aanvulling. In meer dan 74% van alle CV’s staan namelijk onwaarheden. Dat zijn zowel kleine vergissingen (bijvoorbeeld in een datum) als keiharde leugens. In dat laatste geval kan dit grote schade tot gevolg hebben. Denk aan imagoschade, financiële schade of zelfs persoonlijke schade als we kijken naar de zorgsector. Uit onderzoek van onze partner Validata Group blijkt dat 10 tot 15% van de CV’s een echte onwaarheid bevat.

### Datavalidatie: efficiënt en geautomatiseerd

We zien dat steeds meer bedrijven het checken en verifieren van gegevens en data (bijvoorbeeld hoogst genoten opleiding of een VOG) serieuzer (gaan) benaderen. Het is belangrijk dat gegevens kloppen om een juist oordeel te kunnen vellen over de integriteit van iemand. Er zijn bedrijven die zelf op jaarbasis grote aantallen sollicitanten en medewerkers handmatig controleren. Deze bedrijven maken nu vaak de overstap naar een veel efficiënter, geautomatiseerd en volledig digitaal proces. Veel data kan namelijk automatisch en digitaal opgevraagd en gecheckt worden bij bijvoorbeeld overheidsinstanties als DUO. Hierdoor wordt de time-to-hire geminimaliseerd. Dit heeft een positieve invloed op bijbehorende kosten.

### Aandacht voor privacywetgeving

Net als bij screening moet u ook bij datavalidatie rekening houden met privacy. Er moet een gerechtvaardigd belang zijn om een screening of datavalidatie uit te voeren. Onder andere de eis van proportionaliteit speelt een rol. Dit betekent dat informatie die wordt gecheckt – en waarvoor inbreuk wordt gemaakt op iemands privacy – in verhouding dient te staan tot de functie die de persoon gaat bekleden.

### Samenwerking Hoffmann met CV-OK

CV-OK is een label van onze partner Validata Group, specialist in het ‘online’ checken van gegevens van personen en bedrijven. Deze samenwerking is ervoor bedoeld om onze opdrachtgevers een laagdrempelig online proces te kunnen bieden. Bij dit online proces worden alle persoonsgegevens, relevant voor een datavalidatie, snel en veilig geverifieerd. Binnen 3 tot 5 werkdagen ligt er een rapport klaar.

**BIJDRAGE DOOR BART JEROEN BOITEN VAN ONZE NETWERKPARTNER CAPRA ADVOCATEN**

# Mag iedere ziekenhuismedewerker het patiëntendossier van Barbie inzien?

De realityster Barbie werd een paar maanden geleden in het ziekenhuis opgenomen. Wat bleek? Opvallend veel medewerkers keken in haar medisch dossier, het elektronisch patiëntendossier (EPD). Dus volgde nogmaals een discussie over de regels en de beveiliging rondom het EPD. Ik neem u graag mee naar een recente uitspraak van het Gerechtshof Amsterdam. Daarin stond de vraag centraal of een EPD mag worden ingezien. Deze uitspraak heeft ook gevolgen voor ambtelijke werkgevers in de zorg.

### Casus: ontslag op staande voet …

Een medewerkster van een ziekenhuis was op staande voet ontslagen na het onterecht inzien van een EPD. Sinds 2001 werkte zij als secretaresse in het ziekenhuis. Het ziekenhuis heeft een interne gedragscode over het gebruik van het EPD, omdat daar onder andere vertrouwelijke persoonsgegevens en medische gegevens van patiënten in staan. In de gedragscode staat ook duidelijk dat het onterecht inzien van patiëntengegevens leidt tot arbeidsrechtelijke maatregelen.

### … na 2 keer onterecht kijken in een EPD

In 2013 gaat het voor het eerst mis bij deze medewerkster. Zij kan de verleiding kennelijk niet weerstaan en bekijkt een EPD. Ze krijgt hiervoor een waarschuwing. Daarbij wordt duidelijk aangegeven dat er zwaardere arbeidsrechtelijke maatregelen volgen bij herhaling. Toch gaat het in 2017 opnieuw mis. De medewerkster bekijkt meerdere keren onterecht het dossier van een patiënt. Het ziekenhuis ontslaat haar op staande voet. En de kantonrechter geeft het ziekenhuis gelijk. Het betoog over een mogelijke vergissing wordt niet geloofwaardig geacht.

### Uitspraak van het Gerechtshof Amsterdam

Het Hof oordeelt in haar uitspraak van 6 februari 2018 ook dat het ontslag op staande voet rechtsgeldig is. Het Hof kent ook geen transitievergoeding toe, omdat het ontslag een gevolg is van ernstig verwijtbaar handelen of nalaten. De medewerkster was namelijk bekend met de gedragscode. Een gedragscode die volgens het Hof ingebed is in de cultuur van het ziekenhuis en regelmatig wordt besproken op de werkvloer. De aangevoerde persoonlijke omstandigheden doen hier niets aan af. Juist een medewerkster die al zo lang in dienst is zou moeten weten dat ze uiterst zorgvuldig met vertrouwelijke gegevens in een EPD moet omgaan. Bovendien had ze al een waarschuwing gehad.

### Vervolgvraag: mag een ambtenaar een EPD inzien?

Zou de hoogste ambtenarenrechter, de Centrale Raad van Beroep, deze vraag hetzelfde hebben beantwoord? Ook in de zorgsector werken immers (nog) ambtenaren. Bij de Centrale Raad van Beroep is echter nog nooit een uitspraak zoals in de casus hiervoor ter toetsing voorgelegd. Toch durf ik te stellen dat de Centrale Raad van Beroep nog strikter zou toetsen dan in de besproken casus. Al in 2013 oordeelde de Raad dat een ambtenaar altijd een eigen verantwoordelijkheid heeft als het gaat om omgaan met vertrouwelijke gegevens. Het ging over een vergelijkbare situatie als bij het inzien van een EPD: een ambtenaar bij een gemeente deed niet-functionele raadplegingen in bestanden met vertrouwelijke persoonsgegevens. De ambtenaar stelde dat hij niet of niet in toereikende mate op de hoogte was gesteld van de geldende gedragsregels. De Raad verwees naar de ingevoerde gedragscode die op intranet bekend was gemaakt. En weet u wat opvallend was? De Raad gaf aan dat de betrokken ambtenaar had moeten begrijpen dat hij over de grenzen van het toelaatbare ging bij niet-functionele raadplegingen in bestanden met vertrouwelijke persoonsgegevens. Zelfs als de werkgever hem daarover niet zou hebben voorgelicht. Het strafontslag (ontslag op staande voet in het ambtenarenrecht) bleef in stand.

### Soortgelijke casussen voor ambtelijke werkgevers in de zorg

De rechtspositie van een groot aantal ambtenaren gaat veranderen. Het formele procesrecht verandert. Dit betekent dat de meeste ambtenaren gaan vallen onder de werking van het private arbeidsrecht: ze krijgen een tweezijdige arbeidsovereenkomst. Het gevolg hiervan is dat een geschil rondom de arbeidsovereenkomst in de toekomst bij een civiele rechter komt. De bestuursrechter is niet langer bevoegd bij een tweezijdige arbeidsovereenkomst. De civiele rechter toetst binnen het ontwikkelde toetsingskader binnen het civiele recht. Zoals in de casus van de ziekenhuismedewerkster ook het geval was.

### Aanbeveling: zorg voor een actueel intern reglement

De civiele rechter hecht veel waarde aan de voorlichting van medewerkers. Het moet duidelijk zijn voor medewerkers wat de regels zijn en wat de consequenties van het overtreden van de regels zijn. Zorg er daarom ook voor dat in uw reglement duidelijk staat dat medewerkers niet onbevoegd medische gegevens mogen bekijken. En wat als het toch gebeurt? Schrijf duidelijk op wat de consequenties zijn. Deze eisen lijken verder te gaan dan de algemene waarschuwing die volgens de bestuursrechter voldoende kan zijn.

### En Barbie dan?

Mocht iedere medewerker van het ziekenhuis haar EPD inzien? Een duidelijk ‘nee’ is het antwoord. Want eens een realityster betekent niet altijd een realityster. De recente gebeurtenissen hebben laten zien dat een organisatie negatief in de publiciteit kan komen als achteraf wordt vastgesteld dat een EPD ten onrechte is ingezien. Pas regelmatig uw reglementen aan om deze te actualiseren en bespreek dit met uw medewerkers. Vooral voor werkgevers die nu nog onder het ambtenarenrecht vallen is dat zeer aan te bevelen.

# Risicomanagement in 7 stappen

**In ons dagelijks leven hebben we voortdurend te maken met risico's. Ga ik met code oranje de weg op, of niet? Sluit ik een begrafenisverzekering af, of niet? Bewust of onbewust maken we een afweging hoe we met die risico's omgaan. Hoe groot is het risico en wat is de impact als het misgaat? Dezelfde vraag staat centraal bij risicomanagement. Fred Teeven van adviesbureau Verinq gaf in april een lezing tijdens het seminar Bedrijfsfraude & Risicomanagement van Fraude.nl. Om risico's in kaart te brengen en te analyseren onderscheidt Teeven 7 stappen. In dit artikel vatten we ze voor u samen.**

*Stap 1: wat kan er misgaan?*
U begint met een hele algemene inventarisatie van de risico's. Die risico's zijn afhankelijk van bijvoorbeeld de grootte van uw bedrijf en van uw branche. De volgende stappen helpen u om de risico's af te wegen.

*Stap 2: hoe groot is de kans dat het misgaat?*
Dit is een inschatting die u als organisatie maakt. Waar mogelijk op basis van gegevens die u heeft over het verleden of gegevens uit uw branche. Voorbeelden: Hoe groot is de kans dat een medewerker fraude pleegt? Hoe groot is de kans dat u een product moet terugroepen? Hoe groot is de kans dat u negatief in het nieuws komt door een fout van een bestuurder?

*We kunnen risico's beheersen in onze organisaties. Maar risico's uitsluiten is bijna onmogelijk.*

*Stap 3: wat is de verwachte materiële en immateriële schade als het misgaat?*
Mondt een risico uit in een incident of crisis? Dan hebben de consequenties vaak grote impact. Denk bijvoorbeeld aan bedrijfs- en organisatieprocessen die verstoord raken. Of in sommige gevallen zelfs slachtoffers. Maar een risico kan ook een kleine impact hebben.

*Stap 4: hoe kunnen we voorkomen dat het misgaat?*
U denkt na over de maatregelen die u kunt nemen om het risico kleiner te maken. Een actueel voorbeeld is de software van banken waarmee zij nu rekeningnummer en naam van de rekeninghouder checken. Op die manier wordt de kans op een foutieve overboeking kleiner.

*Stap 5: wat kosten de maatregelen en wat is het waard om het risico te beheersen?*
Natuurlijk brengen die maatregelen om risico's te beheersen kosten met zich mee. Is het dat u waard? Misschien neemt u sommige risico's wel voor lief. Bijvoorbeeld bij een risico dat zich hoogstwaarschijnlijk niet voordoet en een gemiddelde impact heeft.

*Stap 6: welke maatregelen treffen we om het risico te beheersen of af te wenden?*
U weet nu hoe groot de kans is dat het misgaat. U heeft ook een inschatting gemaakt van de impact. En u weet wat de eventuele kosten zijn. Op basis van die drie variabelen kunt u een betere beslissing nemen over wel of geen maatregelen. U weegt alle plussen en minnen tegen elkaar af.

*Stap 7: wat doen we als het toch misgaat?*
We kunnen risico's beheersen in onze organisaties. Maar risico's uitsluiten is bijna onmogelijk. Goed dus om ook na te denken over wat u doet als het toch misgaat. Als het risico misschien zelfs uitmondt in een crisis. Denk aan incident- en crisismanagement.

*Fraude.nl is een samenwerking tussen Lexence, Hoffmann & GGN. Een unieke bundeling van drie disciplines: juridische ondersteuning, onderzoek en asset tracing & recovery onder één dak.*

Hoffmann-Tips voor bedrijfsleven en publieke sector is een periodieke uitgave van

Hoffmann

Bezoekadres: Luidsprekerstraat 10, 1322 AX ALMERE
Postadres: Postbus 60090, 1320 AB ALMERE
Telefoon: 088 - 298 6600
info@hoffmann.nl - www.hoffmann.nl