Vijf vragen aan

# Wouter Bas van der Vegt

9 november 2017

## 1. Wie is Wouter Bas van der Vegt en welke expertise heb je?

Een bevlogen en gepassioneerde privacy- en securityprofessional. Vanuit Randstad Holding help ik met veel plezier de Data Protection Officers en Information Security Officers in de verschillende landen de privacy- en securityrisico's van onze organisatie in kaart te brengen en te beheersen. Een uitdagende rol waarin ik dagelijks zoek naar de juiste balans. Randstad verwerkt veel persoonsgegevens die de kern van onze business raken en waarbij we continu rekening houden met de belangen van alle betrokkenen. Het risicomanagement en (nood)scenariodenken vanuit mijn dagelijks leven is zelfs een belangrijk onderdeel van mijn andere passie, zeezeilen!

## 2. Waarom ben je actief geworden in de kennisgroepen Cybersecurity en Privacy?

Ongeveer zeven jaar geleden waren cybersecurity en privacy thema's die nog relatief beperkt op de maatschappelijke en bestuurlijke agenda stonden. Ondertussen ontstond onder meer door mobiele mogelijkheden, social media en cloudoplossingen een exponentiële versnelling in de digitale transitie van de samenleving en organisaties. Vanuit mijn interesse voor de kansen van deze ontwikkelingen, vond ik dat er ook meer aandacht moest komen voor de keerzijde, namelijk de aan deze ontwikkelingen verbonden risico's. Ik heb mij toen aangemeld als lid van de kennisgroep Privacy, waarbinnen een NOREA Privacy Impact Assessment werd doorontwikkeld die vervolgens is gepubliceerd. Toen ik een jaar actief was in die kennisgroep, vroeg NOREA een aantal bevlogen IT-auditors, waaronder ondergetekende, een Cybersecurity/Cybercrime-kennisgroep te starten. NOREA-nevenfuncties hebben het voordeel dat je actief bezig bent met het ontwikkelen van direct toepasbare kennis. Dit levert mij meer op dan het eenzijdig volgen van trainingen of seminars. In mijn huidige internationale rol blijkt dit overigens wat lastiger in te plannen, aangezien ik veel op reis ben.

## 3. Wat hoop je te bereiken met deze kennisgroepen?

Ik hoop met deze kennisgroepen kennisdeling te bewerkstelligen. NOREA heeft leden die, zowel intern als extern, als adviseur actief zijn binnen allerlei lagen van publieke en private organisaties. Zij zien dus nieuwe ontwikkelingen, risico's en maatregelen vanuit verschillende perspectieven binnen hun organisatie. Door deze kennis binnen NOREA via de kennisgroepen actief te ontwikkelen en intern en extern actief te delen, ontwikkelt NOREA zich als platform voor kennisdeling. Om dit te bereiken moeten we echter wel willen delen en ons daar als beroepsorganisatie gezamenlijk voor inzetten. We zullen meer vanuit het gezamenlijk belang moeten opereren en samen de hulpmiddelen ontwikkelen die ons allemaal verder brengen. Een bredere inbreng in de kennisgroepen is een essentiële randvoorwaarde.

## 4. Zijn Cybersecurity en Privacy specialismen of twee van de aandachtspunten van een generalist?

De meeste IT-auditors zijn gespecialiseerde generalisten, en dit geldt ook voor de IT-auditors die actief zijn binnen zowel cybersecurity als het privacydomein. Wat ik daarmee bedoel is dat het voor IT-auditors gemeenschappelijke werkgebied van IT-risicomanagement, IT-audit en IT-governance erg breed en dus generalistisch is. Zeker nu digitalisering ingrijpt op bijna alle processen in een organisatie. Maar gezien de snelheid van ontwikkelingen in cybersecurity en het privacydomein kun je alleen advies leveren dat echt toegevoegde waarde heeft als je ook werkelijk verstand van de actuele stand van zaken hebt. Om je vak serieus uit te kunnen oefenen, ontkom je niet aan een vorm van specialisatie, ofwel op het gebied van processen of een bepaalde markt, dan wel op een inhoudelijk onderwerp zoals cybersecurity of privacy. Daarbij is het, ondanks het specialisme, noodzakelijk de beperkingen van de eigen kennis te onderkennen en tijdig echte (super)specialisten zoals *ethical hackers* of juristen in te zetten. Door de generalistische inslag van de IT-auditor, kunnen wij de uitkomsten van dergelijke werkzaamheden weer naar het bredere kader van de organisatie vertalen.

## 5. Wat is je belangrijkste boodschap voor je collega-RE's?

Leden moeten een actieve rol spelen – en daar bij voorkeur van hun werkgever de ruimte voor krijgen om het vak te ontwikkelen. Een compendium of hulpmiddelen ontwikkelen kost tijd en als de last op een kleine groep collega's rust, is de kwaliteit en snelheid van opleveren lager dan wanneer er door een brede laag IT-auditors zaken worden ontwikkeld. Ook zullen we meer met andere partijen verbinding moeten

zoeken. We zullen ons nog meer moeten gaan ontwikkelen als business-partners, dus niet alleen risico's inventariseren, maar ook praktische adviezen geven en richting geven bij implementatie van die adviezen. Nu zullen veel IT-auditors denken (en misschien ook uitspreken): 'dat doen we toch al door met behulp van risicoanalyse-modellen en control-frameworks uit te leggen wat de business moet doen'. Maar daar zit de crux: de business-stakeholders spreken vaak onze taal niet en het is ze niet altijd duidelijk wat wij bedoelen. De geformuleerde risico's worden als theoretisch gezien en maatregelen als niet concreet. Daardoor bestaat zelfs de perceptie dat IT-auditors, net als andere compliance-gerelateerde beroepen, een remmende factor zijn. Begrip van de context van de organisatie in relatie tot de geïdentificeerde risico's (wat is de typologie, wat is de risicotolerantie, wat is normaal in de markt waarin een organisatie opereert?) en zeker ook voorgestelde maatregelen (wat werkt wel en wat niet in de organisatiecultuur?) verdient meer aandacht. Dit gebeurde vroeger in de IT-auditopleidingen door te onderwijzen in het vak AO/IC, wat een goede leerschool was. Dit onderwerp zou in de huidige opleiding meer aandacht moeten krijgen, maar ook meer moeten worden toegespitst op de huidige digitale samenleving. Ook de snelheid van ontwikkelingen en bijbehorende concepten als Agile en DevOps verdienen meer aandacht. Wellicht moeten we ons zelfs afvragen of het woord IT- (of het soms zelfs nog gebruikte EDP-)auditor nog wel van deze tijd is.


## Wouter Bas van der Vegt | Group Data Protection & Information Security Officer bij *Randstad Holding*

Privé: Gehuwd, Zeiler en Koker  Woont: Aan de Zuid Hollandse Delta