LEIDRAAD IT-RISICO'S VOLMACHT EN HOE TE KIJKEN NAAR UITBESTEDING

In september 2021 kwam de nieuwe Leidraad IT-risico's Volmacht uit. NVGA en het Verbond van Verzekeraars kregen veel vragen vanuit zowel verzekeraars als gevolmachtigden over de IT-risico's en hebben daarom deze leidraad opgesteld. De leidraad geeft richting aan hoe om te gaan met de risico's van IT en biedt veel houvast. Maar wat betekent deze leidraad voor de uitbesteding van de IT en de rol van de gevolmachtigde en de verzekeraar?

Volmachtdrieluik
In dit drieluik staan we stil bij een aantal nieuwe ontwikkelingen op de volmachtmarkt. In het eerste artikel stonden de nieuwe poolovereenkomst en de nieuwe samenwerkingsovereenkomst centraal. In dit artikel is de aandacht gericht op de Leidraad IT-risico's Volmacht. In een volgend artikel zal de POG-leidraad aan bod komen.

De hele leidraad is te vinden op: www.verzekeraars.nl/media/9338/leidraad-it-risicos-volmacht-september-2021.pdf. In dit artikel staat niet zozeer de inhoud van de leidraad centraal. Wat is benoemd daarin is waardevol en nuttig. Iedereen die bezig is met risico's, risicomitigerende maatregelen en gewoon met gezond verstand aan het werk is, kan veel hebben aan de gestructureerde informatie in deze leidraad. Dit artikel gaat vooral in op de koppeling die wordt gemaakt tussen uitbesteding van IT door een gevolmachtigde en de uitbestedingsrol van de verzekeraar.

Uitbesteding van IT en uitbesteding als volmachtgever

Met deze koppeling heb ik wat moeite. Door het publiceren van deze leidraad en de gekozen woorden, *lijkt* het of IT onder de uitbestedingsovereenkomst van de verzekeraar met de gevolmachtigde valt. Er staat namelijk:

'De regelgeving kent open normen waardoor iedere verzekeraar een eigen beleid heeft voor beheersing van IT-risico's. Om de implementatie hiervan in de volmachtmarkt te ondersteunen, is deze leidraad opgesteld. Het biedt handvatten

voor een praktische invulling, die geborgd is in het Werkprogramma Risicobeheersing.'

Door het koppelen van 'het eigen beleid van de verzekeraar' aan 'het ondersteunen van de implementatie hiervan', en dan ook nog te verwijzen naar het werkprogramma, wordt in ieder geval de indruk gewekt dat het hier om uitbesteding gaat van verzekeraar richting gevolmachtigde richting externe IT-leverancier.
Verzekeraars moeten zorgen dat ze voldoen aan de regels van beheerste en integere bedrijfsvoering voor de processen die ze uitbesteden aan gevolmachtigden. Wat besteden ze nu exact uit? Dat zijn de primaire processen zoals vastgelegd in de modelvolmacht. Dat zijn:

Er is geen wet- en regelgeving die voorschrijft hoe automatisering in het specifieke kanaal van gevolmachtigden eruit moet zien

- het zelfstandig ondertekenen van polissen en van alle overige stukken die betrekking hebben op in deze volmacht genoemde handelingen;
- het ontvangen en verrekenen van – alsmede het kwijting geven voor – premies en alle overige gelden wegens aanspraken van de ondergetekende, voortspruitende uit – of verband houdende met – gesloten verzekeringen;
- het meewerken tot wijziging, verlenging of opheffing van gesloten verzekeringen;
- het toezeggen of geven van vermindering, restitutie of kwijtschelding van premies en van gelden die betrekking hebben op alle overige aanspraken van de ondergetekende;
- het van of namens verzekerden in ontvangst nemen van mededelingen;
- het meewerken tot vaststelling van schaden en de omvang daarvan, het regelen, erkennen en betalen van schaden, alsmede het in der minne (door middel van dading of anderszins) treffen van schikkingen in verband met schaden en alle andere aanspraken tegen de ondergetekende;
- het in rechte betwisten van alle aanspraken tegen de ondergetekende;
- het aanhangig maken van rechtsvorderingen ter uitoefening van enig aan de ondergetekende als verzekeraar toekomend recht, het nemen van alle maatregelen die de gevolmachtigde voor een goede procesvoering nodig acht, het meewerken bij – of toestemmen in – het voeren van processen waarbij het belang van de ondergetekende betrokken is;
- het onderwerpen van alle geschillen aan de beslissing van scheidsmannen alsmede het verlenen van zijn/haar medewerking in het scheidsrechterlijk geding; waarbij alle desbetreffende handelingen en verbintenissen van de genoemde gevolmachtigde voor de ondergetekende zullen gelden, geheel als waren zij door hem verricht of aangegaan.

Voorgaande opsomming is wat een verzekeraar uitbesteedt en waar hij vervolgens in overeenstemming met de wet op toe kan zien. Ook geldt bij deze taken dat hij van de gevolmachtigde mag eisen, wanneer deze dat proces weer verder uitbesteedt, dat aan bepaalde normen wordt voldaan. IT is niet een proces wat de verzekeraar uitbesteedt aan de gevolmachtigde, net zomin als HR-activiteiten of het versturen van post of het laten verzorgen van de catering van het bedrijf of welke standaardactiviteiten van een bedrijf dan ook. Er zijn verzekeraars die hier anders over denken en vinden dat IT als middel om de primair uitbestede processen uit te kunnen voeren, ook valt onder de uitbesteding als volmachtgever. Ik begrijp wel waarom een verzekeraar meer grip wil op dit onderdeel bij de gevolmachtigd agent. IT is inmiddels een wezenlijk onderdeel van het goed kunnen uitvoeren van de kernprocessen die zijn uitbesteed. Dan mogen er ook (terecht) meer eisen worden gesteld aan IT bij gevolmachtigden. Maar binnen de Good Practice van DNB wordt nergens letterlijk iets gezegd over IT. Dit betekent dat hoewel IT een zeer belangrijke rol vervult in de hele keten, er niet direct vanuit wet- en regelgeving enige vorm of inhoud wordt gegeven aan de automatisering in het kanaal van gevolmachtigden *via* verzekeraars.

De elf principes van informatiebeveiliging

Natuurlijk heeft de gevolmachtigde zijn eigen zelfstandige plicht om te voldoen aan de elf principes van informatiebeveiliging van de AFM. Deze kun je terugvinden op: https://www.afm.nl/nl-nl/nieuws/2019/dec/principes-informatiebeveiliging. Deze elf principes zijn vrij in te vullen voor iedere onderneming, dus ook voor de gevolmachtigd agent. Wel moet het beleid er zijn en moet er goed worden nagedacht over het verminderen van de risico's van een incident en het beperken van de impact als een incident zich voordoet. Dat is het hoofddoel van de principes. Als hij onderdelen uitbesteedt, moet een gevolmachtigde dit beschrijven en aan kunnen tonen door interne en externe controles. Dit is vastgelegd in de onderdelen in het werkprogramma onder het kopje Automatisering. De elf principes zijn:

1. Beleid: een actueel informatiebeveiligingsbeleid beschrijft een samenhangend geheel van maatregelen, procedures en processen waarmee informatiebeveiligingsrisico's worden beheerst.
2. Governance: de onderneming richt een governancestructuur in die effectieve informatiebeveiliging mogelijk maakt.
3. Identificeren van dreigingen en beoordelen van risico's: informatiebeveiliging is ingericht op basis van een actueel inzicht in bestaande dreigingen en risico's, de potentiële impact van bestaande dreigingen op de onderneming en de risicobereidheid van de onderneming.
4. Mensen en cultuur: de onderneming onderkent het risico van menselijk handelen voor informatiebeveiliging en creëert en ondersteunt een cultuur waarin medewerkers zich bewust zijn van het risico op informatiebeveiligingsincidenten en hierover open communiceren.
5. Technologie: bij de implementatie en het onderhoud van systemen wordt het uitgangspunt 'secure by design' toegepast.
6. Processen: de inrichting van bedrijfsprocessen waarborgt de beschikbaarheid, integriteit en vertrouwelijkheid van processen

»

en de hierin gebruikte systemen.
7. Fysieke beveiliging: het ontwerp en de inrichting van de faciliteiten en apparatuur van de onderneming zijn in lijn met de eisen aan informatiebeveiliging.
8. Data: tijdens de volledige levenscyclus van data en informatie zijn maatregelen getroffen om te voldoen aan de relevante beveiligingseisen.
9. Respons en herstel: de onderneming is voorbereid op informatiebeveiligingsincidenten om de impact hiervan op de bedrijfsvoering van de onderneming te beperken. Wanneer zich een informatiebeveiligingsincident voordoet, neemt de onderneming tijd en doeltreffende respons- en herstelmaatregelen.
10. Uitbesteding: de onderneming is verantwoordelijk voor de informatiebeveiliging van uitbestede processen en systemen.
11. Ketenperspectief: de onderneming past een integrale ketenbenadering toe bij het bepalen van informatiebeveiligingsrisico's en de benodigde maatregelen.

Maar principe 10 Uitbesteding moet niet worden verward met de uitbesteding zoals volmachtgevers en volmachtnemers met elkaar vastleggen in de samenwerkingsovereenkomst. Daarin gaat het om toezicht op het wéér verder uitbesteden van taken aan een derde. Bijvoorbeeld schaderegeling. Een verzekeraar besteedt schaderegeling uit aan de gevolmachtigde en vervolgens besteedt die deze taak weer uit aan een ander schaderegelingsbureau. Dat is uitbesteding waarop de verzekeraar toestemming moet geven (of afkeuren). Immers, hij besteedt dit niet voor niets aan de gevolmachtigde uit. Als die vervolgens niet het primaire proces zelf gaat uitvoeren, wordt het onderuitbesteding en daar moet de verzekeraar wat van kunnen vinden. Overigens vind ik ook dat een verzekeraar dit tegen moet kunnen houden als het een partij betreft die de verzekeraar niet wenst, of als de verzekeraar in zijn eigen beleid heeft bepaald dat dit niet mag.

Controle op IT-uitbesteding

Besteedt een gevolmachtigde zijn IT-beheer uit, dan mag daar natuurlijk controle op zijn. Welke controle en hoe hierover gerapporteerd wordt, dat moeten gevolmachtigde en verzekeraar met elkaar afspreken. Zoals we dat bijvoorbeeld in de markt vastleggen in het werkprogramma. Het gaat hier dus niet om de uitbestedingsrelatie volmacht–volmachtgever en dus het specifiek kunnen voorschrijven van richtlijnen door verzekeraars. Dat moet je ook helemaal niet willen als verzekeraar. Het is de zelfstandige verplichting van de gevolmachtigde om dit goed te doen en volgens de wet. Daarnaast doet de gevolmachtigde dit natuurlijk ook vanuit haar eigen risicobesef en behoefte aan bedrijfscontinuïteit.

De gevolmachtigde moet voldoen aan de elf principes van informatiebeveiliging van de AFM

Richtlijn 2009/138/EG

Vaak verwijzen verzekeraars naar artikel 49 van Richtlijn 2009/138/EG. Daarin staat een definitie van uitbesteding: een overeenkomst van om het even welke vorm tussen een verzekerings- of herverzekeringsonderneming en een al dan niet onder toezicht staande dienstverlener, op grond waarvan deze dienstverlener hetzij rechtstreeks hetzij door middel van onderuitbesteding een proces, een dienst of een activiteit uitvoert, die anders door de verzekerings- of herverzekeringsonderneming zelf zou worden uitgevoerd. Uiteindelijk gaat het in deze richtlijn met name om het faciliteren van toegang van de toezichthouders op de uitbestedingsrelatie en bij de gevolmachtigde zelf. En die toegang heeft de AFM. Nergens wordt expliciet inhoud gegeven aan wat wordt bedoeld met 'hetzij door middel van onderuitbesteding een proces, een dienst of een activiteit uitvoert die anders door de verzekerings- of herverzekeringsonderneming zelf zou worden uitgevoerd'. Dus het kan zijn dat de verzekeraar die IT wel als uitbesteding ziet, hier wat anders van vindt. Het laatste woord is er vast nog niet over gezegd, ik ben benieuwd waar het heen gaat.

Voor nu is de leidraad IT een zeer handig en informatief middel voor een gevolmachtigde. Ik raad het iedereen aan om deze eens goed door te nemen. Maar waak er dus voor om IT niet te scharen onder een uitbesteed proces van de verzekeraar aan de gevolmachtigde. Zorg voor een goede inrichting van je IT-uitbesteding in je eigen organisatie en pak dit professioneel aan, rapporteer hierover via het werkprogramma. Doe wat je als professioneel bedrijf moet doen, maar zorg er ook voor dat je hierin zelf in de regie blijft en de verzekeraar niet laat bepalen hoe je omgaat met je eigen uitbestede processen. ●

Drs. M.A. (Mieke) Dadema (Msc)
De auteur is eigenaar van Draad consultancy BV en tevens lid van de redactieraad van *de Beursbengel.*