DOOR JANNIE BENEDICTUS : FOTOGRAFIE PETER STRELITSKI

Kan ik ook teveel van de klant weten?

De wetgeving rondom privacy verandert razendsnel. Elk bedrijf dat persoonsgegevens verwerkt, heeft er mee te maken. En tussenpersonen zitten op bergen persoonsgegevens. Maar waar moet je als intermediair op letten? Wanneer moet je klantdossiers vernietigen? En controleert de verzekeraar het intermediair of is het andersom? Die vragen stelt Roy van den Anker, operationeel directeur bij MultiSafe. Maar kristalheldere antwoorden... die zijn er nog niet.

HET CONSULT

Het Consult is een initiatief van am:magazine en Bureau D & O. Intermediairs kunnen hun vraag in een interactieve sessie voorleggen aan een panel dat in samenstelling wisselt al naar gelang de aard van de vraag. De redactie van am:magazine legt het gesprek vast in een artikel. De panelleden houden de vinger aan de pols bij het intermediair. Meedoen? Stuur een mail met uw vraag naar redactie@amweb.nl.

Roy van den Anker is operationeel directeur bij makelaar MultiSafe in Huis ter Heide en privacy is een van de onderwerpen op zijn volle bordje. Het onderwerp komt dagelijks voorbij. Neem een werkgever die in het kader van het vaststellen van mogelijk eigenrisicodragerschap het hele personeelsbestand inclusief ziektes op de mail zet. Is dat acceptabel? Of neem een afwijzing voor een AOV op grond van medische redenen: die klantgegevens wil je graag onthouden om de klant de keer daarop weer goed van dienst te kunnen zijn, maar mag dat ook? Of moet je ze vernietigen?

MOEHEID

Van den Anker snijdt daarmee geen populair vraagstuk aan. Panellid Thomas Heuperman, jurist bij D & O, krijgt regelmatig vragen van

‘HET GEVAAR DREIGT DAT ER IN DEZE BRANCHE EEN MACHTIGINGSCULTUUR ONTSTAAT’

intermediairs over de wet bescherming persoonsgegevens. “Ze worden zich bewust van het feit dat ze als financieel dienstverlener op veel data zitten. Maar er is ook moeheid onder het intermediair om zich met dit vraagstuk bezig te houden. Ze hebben al zoveel op hun bord.”

Panellid Bettie Hoogsteen, beleidsadviseur bij Adfiz, haakt in. “Wij zien bij het intermediair alle bereidheid om zorgvuldig met klantgegevens om te gaan. Onze leden begrijpen dat verzekeraars dat ook moeten doen. Tegelijk is het lastig dat verzekeraars klantgegevens niet altijd meer delen. Er moet dan op grond van privacyregelgeving eerst een machtiging van de klant komen. Neem een kopie uitkeringsbericht van een AOV. Je wilt je klant bijstaan als die arbeidsongeschikt wordt, maar daarvoor moet je wel bij die gegevens kunnen. En dan stelt de verzekeraar een machtiging verplicht.”

Volgens Hoogsteen dreigt het gevaar van een machtigingscultuur. “Dat is onwenselijk. Het strookt niet met de gedachte dat de adviseur een gezond tegenwicht moet bieden richting de verzekeraar. Het beschikken over alle informatie is daarbij een kritische succesfactor.” Hoogsteen zegt niet dat verzekeraars zich verschuilen achter privacywetgeving om meer grip te krijgen op de klant. “Het is een oprechte zorg van verzekeraars, ze willen het heel goed doen. Maar soms schieten ze door.”

ZOVEEL MOGELIJK

Panellid en advocaat Rik Geurts heeft de ervaring dat verzekeraars graag zoveel mogelijk gegevens verzamelen. “Wij komen dat vaker tegen bij zorgverzekeraars. In de privacywetgeving gaat het er echter om welke informatie noodzakelijk is voor het doel dat je wilt bereiken. Dat moet je steeds in je achterhoofd houden. Dus in jullie branche: wat heb je nou echt nodig om de klant goed te kunnen bedienen?” Van den Anker herkent die informatiebehoefte van verzekeraars. “In arbeidsongeschiktheidsdossiers wordt soms allerlei informatie aan de klant gevraagd die eigenlijk niets met de situatie te maken heeft. Ik vind dat wij als adviseurs in zo’n geval het belang van de klant moeten dienen.” Privacy-expert Francis Joung: “Dat zou ik zeker als onderdeel van mijn dienstverlening inzetten. Je kunt best tegen de verzekeraar zeggen: gelet op wat er speelt, is wat je vraagt wel heel overmatig en maak je inbreuk op de privacy van mijn klant.”

MELDEN

De vragen van Van den Anker zijn actueel want er verandert veel in de privacyregelgeving: de boetes zijn gigantisch verhoogd en de meldplicht op datalekken is in werking getreden. Wie persoonsgegevens verwerkt, moet de verwerking nu nog melden bij de Autoriteit Persoonsgegevens, totdat in 2018 de richtlijn AVG rechtstreekse werking krijgt (zie kader). Het panel schat zo in dat niet alle tussenpersonen zich netjes bij de Autoriteit hebben gemeld. Heuperman: “Dat is jammer, want zo’n melding creëert in ieder geval bewustzijn en zorgt dat je er over gaat nadenken.” De meldplicht wordt opgeheven wanneer per 2018 de nieuwe richtlijn van toepassing wordt. Geurts: “De nieuwe regels verlangen dat je veel actiever op privacy gaat sturen. Het gaat naar een documentatieplicht.” Joung vult aan: “Aantoonbaarheid wordt heel belangrijk. Je zult onder meer een privacybeleid moeten hebben waarin staat uitgeschreven hoe je met de gegevens omgaat, ook voor je personeel.” Van den Anker zegt daar al mee bezig te zijn.

PRIVACYREGELGEVING

De Algemene Verordening Gegevensbescherming gaat per 25 mei 2018 de Wet bescherming persoonsgegevens vervangen. In 2018 zal iedere organisatie die persoonsgegevens verwerkt, en dus ook het hele intermediaire kanaal, aan de nieuwe eisen moeten voldoen. Het is dan verplicht om een register te hebben met een overzicht van je gegevensverwerkingen. Ook moet je documentatie hebben die beschrijft wat je bedrijf doet om privacy te waarborgen: zowel richting klanten (bijvoorbeeld een privacystatement op de website en in de algemene voorwaarden) als intern (een actief beleid met bijbehorende maatregelen).

Roy van den Anker

Hij vertelt: “Wij hebben huisregels opgesteld. Een voorbeeld: onder ieder bureau staan twee bakjes: een voor waardeloos oud papier en een voor de vertrouwelijke datacontainer die door een gespecialiseerd bedrijf wordt afgevoerd.”

Het panel gaat nog even in op het bewaren van documenten. Geurts: “Je zult de dossiers moeten vernietigen of in ieder geval moeten anonimiseren als de bewaartermijn is verstreken.” Maar gebeurt dat in de praktijk? Adviseurs willen klantgegevens graag bewaren om de klant in een nieuw adviestraject goed van dienst te kunnen zijn. Panellid Heuperman voegt toe: “Bovendien wil je in de toekomst kunnen laten zien dat je een goed advies hebt gegeven. Aan de toezichthouder of in een Kifidprocedure.” Geurts: “De Wet bescherming persoonsgegevens biedt wel enkele uitzonderingsbepalingen, je mag zaken bewaren bijvoorbeeld in geval van claims. Maar nogmaals geldt: wat is echt nodig? Denk daar over na.”

BEWERKERSOVEREENKOMST

Een belangrijk punt in de discussie is de bewerkersovereenkomst die gesloten wordt wanneer een partij het bewerken van persoonsgegevens aan een andere partij uitbesteedt en waarin staat hoe die bewerker met de data moet omgaan. Van den Anker: “Wij hebben bijvoorbeeld zo’n overeenkomst van Anva ontvangen. Die werd direct van toepassing verklaard, middels een negatieve optie. Dat hebben we niet geaccepteerd en we zijn nog in overleg over de juiste formulering.”

LESSONS LEARNED

- **Creëer bewustwording op kantoor: de privacy van klanten is belangrijk.**
- **Een goed financieel adviseur zorgt ervoor dat er door een verzekeraar niet meer aan de klant wordt gevraagd dan nodig is.**
- **Aanmelden bij de Autoriteit Persoonsgegevens is nu nog verplicht.**
- **Maak werk van een extern statement en een intern privacybeleid.**
- **Als je verantwoordelijk bent, zorg dan dat je in de lead bent richting de bewerker.**
- **Agendeer het periodiek opschonen van dossiers en persoonsgegevens.**
- **Zorg dat je persoonlijke gegevens van klanten beveiligd/encrypted verstuurt.**

Eigenlijk gaat het daar meteen al mis, vindt het panel van juristen en privacy-experts. Bij zo’n bewerkersovereenkomst heb je namelijk een verantwoordelijke partij en een bewerker. De eerste partij moet in de lead zijn. In het geval van Anva is MultiSafe de verantwoordelijke partij en zou MultiSafe de inhoud van de overeenkomst moeten opstellen. Datzelfde geldt voor het geval een intermediair samenwerkt met een serviceprovider: de tussenpersoon is verantwoordelijk voor de data en de serviceprovider is bewerker. En dus moet het assurantiekantoor in control zijn en de overeenkomst opstellen. Maar dat gebeurt niet, zegt Van den Anker, want er zijn erg veel tussenpersonen en Anva gaat niet met elke tussenpersoon apart om tafel.
Hier ligt een mooie taak voor de branchevereniging, zo is de stemming aan tafel. Hoogsteen: “We moeten daar met verschillende partijen naar kijken. Absoluut. Maar niet alles is nog duidelijk. Het is niet altijd even makkelijk om vast te stellen wie de bewerker is en wie de verantwoordelijke.” Joung beaamt dat: “De rolverdeling tussen intermediair en verzekeraar is soms wat onduidelijk. Je moet bij elke informatiestroom scherp maken wat je rol en dus je verantwoordelijkheid is.” Hoogsteen: “Maar duidelijk is wel dat bij de gegevensuitwisseling tussen tussenpersoon en verzekeraar, de tussenpersoon de verantwoordelijke is.”

Advocaat Geurts: “In bepaalde gevallen zal de tussenpersoon vanuit zijn rol toezicht moeten houden op de verzekeraar. Hij zal dan in de bewerkersovereenkomst moeten opnemen dat hij met deskundigen mag binnenkomen om te

HET PANEL

Rik Geurts werkt als advocaat bij Van Iersel Luchtman Advocaten en is gespecialiseerd in Intellectueel Eigendom, Informatie Technologie en Privacy. Privacyvraagstukken vormen een groot onderdeel van zijn werk.

Bettie Hoogsteen is beleidsadviseur bij brancheorganisatie Adfiz en houdt zich bezig met tal van vraagstukken op het terrein van de Wft, waaronder ook het dossier vakbekwaamheid. Ze begon in 1989 bij (toen) de NVA.

Francis Joung werkt sinds begin 2016 als senior consultant bij Privacy Management Partners dat bedrijven adviseert over hun privacybeleid. Daarvoor werkte hij bij Achmea en Syntrus Achmea, laatstelijk als Privacy Officer.

Thomas Heuperman is sinds begin 2016 jurist bij Bureau D & O. Hij geeft juridische ondersteuning aan het intermediair op het gebied van de Wft, Wbp, contractenrecht en diverse andere wet- en regelgeving.

kijken wat de verzekeraar met de gegevens van zijn klanten doet." Als voorbeeld noemt Geurts het hypotheekadvies. "Stel: de tussenpersoon vraagt een aantal offertes op bij geldverstrekkers. Dan is de tussenpersoon de verantwoordelijke partij en stuurt hij idealiter alleen aanvragen naar die partijen die een overeenkomst willen sluiten waarin staat dat zij de klantgegevens zullen vernietigen als het niet komt tot een hypotheek." Van den Anker glimlacht. "Nou dat is in onze branche echt nog niet op die manier geregeld." En, weet ook het panel, zo gaat dat gewoon niet. Joung: "Het is een kwestie van bewustwording. Het gaat er steeds om: wat is mijn rol?"

ZIEKE MEDEWERKERS

Van den Anker heeft een actuele casus: op dit moment zijn veel werkgevers met hun adviseurs in gesprek over het WGA eigen risico. "Zieke medewerkers met ballast zijn daarin heel relevant voor het advies. De ene klant stuurt klakkeloos zijn hele personeelsbestand over de mail met alle details, terwijl de andere netjes een inlogcode verstrekt voor een beveiligde omgeving", vertelt hij. Joung waarschuwt meteen: "Als jij als tussenpersoon het medium bepaalt waarlangs een werkgever gegevens gaat sturen, dan ben jij verantwoordelijk. Wees je daar bewust van, accepteer ook niet dat zo'n bestand over de mail komt." Ook Geurts vindt dat tussenpersonen voorzichtig moeten zijn met dergelijke gegevens: "Geef een signaal terug aan de werkgever als je teveel informatie krijgt. Je hoeft niet meer te ontvangen dan wat echt nodig is voor je advies. Een werkgever mag echt geen gedetailleerde medische gegevens verstrekken over werknemers."

Tot slot: wat neemt Van den Anker mee terug naar kantoor in Huis ter Heide? "Mijn grootste eyeopener is dat we in veel gevallen in plaats van bewerker verantwoordelijke zijn. En dat wij dus moeten kijken wat er bij de verzekeraar met de gegevens van ónze klant gebeurt." ■