Foto's: Gerda Horneman

René Mackenbach (Wooncompagnie):

Goede informatiebeveiliging vraagt om een risicobewuste organisatie

Anderhalf jaar geleden ging de handhaving op de AVG van start in de corporatiesector. Maar waar die datum rood omcirkeld stond bij woningcorporaties, werd er maar weinig gezegd over het traject daarna. Want hoe houd je medewerkers bewust en zorg je ervoor dat informatiebeveiliging en privacy blijven leven binnen de organisatie? CorporatieGids Magazine vroeg het aan **René Mackenbach**, Adviseur Kwaliteit en Procesbeheer bij **Wooncompagnie**.

Een van de petten die René draagt bij Wooncompagnie is die van Privacy Officer. Op de vraag hoeveel tijd de functie vergt in vergelijking met anderhalf jaar geleden, vertelt hij: "In de voorbereiding van de AVG ben ik daar natuurlijk erg druk mee geweest. Het onderwerp was voor mij niet helemaal nieuw, omdat ik in eerdere functies te maken heb gehad met de voorloper van de AVG. Inmiddels zit het grootste deel van de tijd in het bewust maken én houden van de organisatie."

Bewuste organisatie

"Goede informatiebeveiliging betekent voor mij hoofdzakelijk dat de organisatie bewust is van de risico's," legt René uit. "Natuurlijk moet je aan de technische kant zaken regelen, zoals autorisaties inregelen en het afschermen van informatie. Maar je moet het menselijke aspect zeker niet onderschatten. Dat betekent bijvoorbeeld de organisatie bewust maken van phishinggevaren, maar ook het uitvoerbaar houden van het beveiligingsbeleid. Je kunt alles wel dichttimmeren en beveiligen, maar dan belemmer je mensen in de uitvoering van hun werk. Je moet daarin de gulden middenweg zien te vinden en begrijpen dat een ingecalculeerd risico soms onvermijdelijk is."

Geen eindpunt

Het bewust houden van medewerkers noemt René de grootste uitdaging qua informatiebeveiliging voor de Noord-Hollanders. "Wat je vaak ziet, is dat een project – zoals de AVG – mensen bezighoudt totdat het geïmplementeerd is. Maar in de praktijk heeft het geen eindpunt. Er volgen continu nieuwe ontwikkelingen waarop je moet inspelen, nieuwe informatie waarmee je moet omgaan en nieuwe zaken waar de organisatie tegenaan loopt. Daar moet je de organisatie in meenemen."

"Een goed voorbeeld daarvan is het recente voorstel van de staatssecretaris om gemeenten de bevoegdheid te geven om betaalachterstanden in te kunnen zien bij onder meer woningcorporaties en zorgverzekeraars. Dat heeft AVG-technisch een behoorlijke impact. Je moet namelijk afspraken maken met de gemeente, maar ook het verwerkingsregister moet hiervoor aangepast worden. Een heel treintje aan veranderingen wordt daardoor in werking gezet."

Eenmeting

Om te kijken waar de organisatie staat omtrent informatiebeveiliging en privacy, heeft Wooncompagnie onlangs een eenmeting laten uitvoeren. René: "We wilden kijken waar we iets meer dan één jaar na de AVG stonden. De eenmeting is uitgevoerd door Audittrail, onze advies en consultancy partner met wie we al geruime tijd samenwerken om aan de vereisten van de AVG te voldoen. Zij hebben een instrument ontwikkeld waarmee we op verschillende onderdelen – zoals datalekken, verantwoording of bewustzijn – kunnen zien hoever we zijn."

Gedachte achter de AVG

Uit deze meting bleek dat het administratieve gedeelte rondom de AVG en informatiebeveiliging nog beter kan bij Wooncompagnie. René herkent zich wel in die resultaten: "Dat heeft te maken met de opzet die wij hebben gehanteerd. Wij hebben de AVG zo opgezet dat we niet honderden regeltjes willen toevoegen, maar juist de gedachte achter de AVG zoveel mogelijk willen volgen. Je gaat om met de gegevens van je huurders, en die wil je zo goed mogelijk behandelen. Dat kan echter betekenen dat sommige dingen nog niet helemaal lopen zoals het moet, zoals het administratief registreren van bepaalde werkwijzen. Daar willen we ons de komende periode op richten. Overigens blijkt deze manier wel enorm goed te werken op andere onderdelen, zoals bewustwording waar we bovengemiddeld hoog scoren."

Oplossingen van de organisatie

Het meenemen van de organisatie bij de implementatie van de AVG was erg belangrijk, stelt René: "We hebben gekeken met de teams die persoonsgegevens verwerken wat het voor hen betekent. Het is daarbij belangrijk dat informatiebeveiliging iets van henzelf wordt. We hebben daarom gekeken naar praktijkcasussen. Op die manier kom ik niet met een setje maatregelen, maar komt vanuit de afdeling de vraag 'mag ik dit nog wel doen in deze situatie'. Zo neem je ze mee in hun eigen scenario's, en worden de oplossingen echt iets van henzelf."

Niet overvoeren

"Daarbij is het belangrijk dat je niet doorslaat in je bewustwordingscampagne," gaat René verder. "Dit jaar hebben wij bijvoorbeeld wat minder focus hierop gelegd, maar in 2020 schroeven we de campagnes weer wat verder op. De reden dat we het niet ieder jaar doen, is omdat je de organisatie ook niet moet overvoeren. Wanneer je iedere maand een herinnering krijgt over phishingsmails of de beveiliging

van een computerscherm, dan sluipt het gevaar erin dat medewerkers na een tijdje denken 'ja, ik weet het nu wel'.

>>

Je kunt alles wel dichttimmeren en beveiligen, maar dan belemmer je mensen in de uitvoering van hun werk.

Je moet het verrassingseffect houden om te zorgen dat het niet averechts werkt."

Een voorbeeld van zo'n verrassingseffect is het gebruik van een Mystery Guest: "Die persoon kwam bij ons op kantoor en keek hoever die kon komen. Dan merk je dat sommige zaken heel goed gaan; de serverruimte werd goed afgeschermd en computerschermen werden afgesloten wanneer iemand van zijn of haar bureau wegliep. Maar je merkt ook dat bepaalde dingen minder goed gaan, zoals het niet aanspreken van een onbekend iemand die het kantoor binnenloopt. Die informatie wordt echter wel ten harte genomen door de organisatie. De medewerkers die bijvoorbeeld vlakbij de ingang zitten, hebben direct hun werkwijze aangepast en gezorgd dat dit niet meer kan gebeuren. Zo zorg je ervoor dat maatregelen echt van de organisatie zijn, en niet bovenaf door iemand worden opgelegd."

Lust en last

Op de vraag of informatiebeveiliging inmiddels als lust of last wordt gezien door de organisatie, vertelt René: "Het is een beetje van beide. Aan de ene kant een last, omdat informatie- en privacywetgeving een beperking opleggen aan de organisatie. Niet alles mag en je moet hier continu op letten. Daarnaast kost het tijd en geld om dit in te regelen en onder de aandacht te houden. Aan de andere kant worden de voordelen wel ingezien. Medewerkers begrijpen de noodzaak en weten dat technisch zaken goed geregeld zijn en er goede handvatten zijn om aan de wetgeving te voldoen. Dat zorgt ervoor dat er geen zwaard van Damocles boven de organisatie hangt, en dat geeft rust."

Digitale bewustwording

"Aandacht besteden aan informatiebeveiliging en privacy blijft ook in de toekomst essentieel," sluit René af. "Daarbij zal digitale bewustwording en bescherming steeds belangrijker worden. Ontwikkelingen als portalen, de cloud en Office 365 zorgen ervoor dat we steeds meer online werken, en het is moeilijk te zien wat soms met gegevens gebeurt en wat de impact is. Daarnaast zal de manier waarop we met bewoners communiceren ook veranderen. We gebruiken nu nog veel e-mail, maar is dat de manier van de toekomst? Vergelijk het met de introductie van aangetekende post voor fysieke brieven en pakketten, dat ontwikkelt zich ook. Door middel van documenten met wachtwoorden, two-way authentification en geavanceerde portalen zal communicatie beter afgeschermd en beveiligd worden." ■