Foto's: Audittrail, Shutterstock

Suzanne van Middelkoop (Audittrail):

Privacybewust werken moet vanzelfsprekend worden

Hoewel de AVG al drie jaar geleden werd ingevoerd, was ongeveer een jaar geleden de deadline van de nieuwe regelgeving. Zijn woningcorporaties inmiddels compliant, of is er slechts een basis gelegd en moeten er nog steeds stappen worden genomen? **Audittrail** deed hier onderzoek naar en CorporatieGids Magazine sprak daarover met Manager Innovatie **Suzanne van Middelkoop**.

Audittrail heeft de afgelopen jaren verschillende corporaties geholpen met de opzet van AVG compliance, legt Suzanne uit. “Vaak was daarbij een nulmeting het startpunt, waardoor helder werd wat de corporatie nog te doen had. We zien nu steeds vaker de overstap van projectopzet naar inbedding in de organisatie. Nu is het zaak voor woningcorporaties om compliant te blijven en de puntjes op de i te zetten.”

Valide resultaten

Op verschillende momenten doet Audittrail onderzoek naar de AVG-volwassenheid van woningcorporaties. “Op Corporatie-Gids LIVE – 16 april van dit jaar – hebben wij een steekproef gehouden onder vijftien corporaties. De resultaten uit die proef onderschrijven het beeld dat uit interne onderzoeken ook naar voren komt.”

Privacybeleid

Zo blijkt dat door de invoering van de AVG woningcorporaties de privacy van haar huurders en medewerkers meer aandacht hebben gegeven, en is door alle corporaties in de steekproef een privacybeleid opgesteld. “Met de invoering van de nieuwe regelgeving is privacybeleid uitgegroeid tot een op zichzelf staand onderwerp,” zegt Suzanne. “Een voetnoot hierbij is wel dat 10 procent van de corporaties geen verantwoordelijke voor het beleid heeft aangewezen. Dat is niet verplicht, maar wel aan te raden. Het is belangrijk – zeker nu we nog in de beginfase zitten van AVG compliance – om iemand aan te wijzen die de samenhang kan bewaken en de verbinding kan leggen tussen verschillende partijen en belangen.”

Herkennen en handelen

Meer stappen zijn er nog te maken rondom datalekken. Zo geeft bijvoorbeeld 47 procent van de corporaties aan moeite te hebben met het herkennen hiervan en weet 36 procent niet hoe het moet handelen bij een datalek. “Omgaan met datalekken is een kwestie van bewustwording,” vertelt Suzanne. “Dit heeft tijd nodig. Mensen zijn niet bewust na ze eenmalig geïnformeerd te hebben. Corporaties doen er daarom goed aan een plan op te stellen en medewerkers blijvend te informeren, voorbeelden te gebruiken en hiervan te leren.”

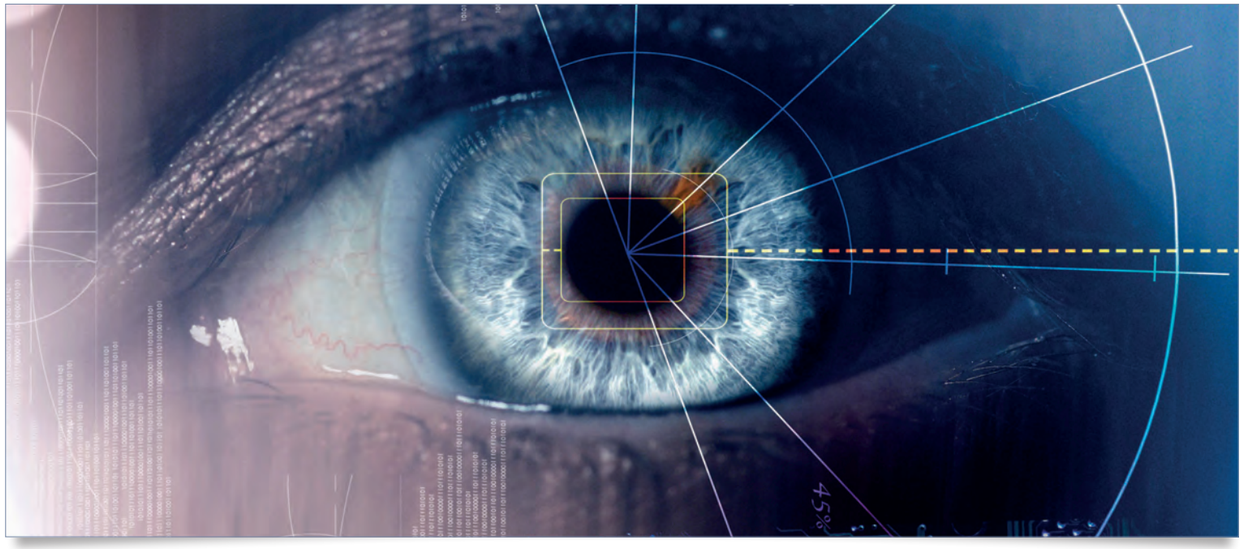
Daarnaast blijkt dat datalekken bij 32 procent van de corporaties niet op de juiste manier geregistreerd worden. “De regels rond het registreren en de bewaartermijnen hiervan zijn vrij expliciet, maar nog niet bij iedereen op het netvlies. Waar vaak wel een registratie wordt bijgehouden van het incident, wordt de opvolging van incidenten nog niet altijd geregistreerd. Ook het naleven van bewaartermijnen of het periodiek evalueren van uitkomsten van datalekken gebeurt nog niet overal.”

Leren van incidenten

Volgens Suzanne zullen tijd en incidenten ervoor zorgen dat datalekken beter worden herkend, aangepakt en geregistreerd. “Woningcorporaties hebben de randvoorwaarden voldoende ingevuld op het moment dat ze een procedure hebben en werken aan het bewustzijn van medewerkers. Verder kun je bijzonder goed leren van de incidenten die voorkomen binnen je organisatie. Een algemene datalek-databank, waarbij je ook de datalekken van andere organisaties kunt zien, zou daarbij ook uitkomst kunnen bieden. Overigens brengt de AP elk kwartaal een rapportage uit over de meest gemelde datalekken. Het versturen van gegevens naar een verkeerd geadresseerde steekt daarin met kop en schouders erbovenuit.”

DPIA

Uit de steekproef blijkt ook dat slechts 25 procent van de corporaties weet wanneer een Data Protection Impact Assessment (DPIA) nodig is en dit ook structureel goed uitvoert. “Een DPIA is een manier om risico’s rondom een verwerking goed in kaart te brengen,” licht Suzanne toe. “Hier bestaan geen vastgestelde richtlijnen voor, maar het moet wel aan een aantal voorwaarden voldoen. Bijvoorbeeld het bevatten van een systematische beschrijving van de gegevensverwerking en een beoordeling van de privacy-risico’s. Wanneer een verwerking een ‘hoog risico’ oplevert, is een DPIA verplicht. Hoewel de AP een aantal handvatten geeft om te bepalen wanneer een verwerking tot een hoog risico gerekend wordt, blijft het een grijs gebied. Omdat corporaties nog niet zo lang bezig zijn met de AVG is het uitvoeren van een DPIA geen dagelijks werk, waardoor het maken van een goede inschatting lastig is.”



Verwerkingenregister

Het verwerkingenregister is bij 88 procent ‘in meer of mindere mate op orde’. “Dat zo’n register nog niet helemaal op orde is, heeft uiteenlopende redenen. Soms zijn nog niet alle processen in kaart gebracht en daarmee nog niet alle verwerkingen. Of er is geconstateerd dat er gegevens teveel worden uitgevraagd, te vroeg in het proces of zonder reden. Dit betekent dat het proces verder onder de loep genomen dient te worden en dataminimalisatie moet worden toegepast.”

Volgens Suzanne is het up-to-date houden van het verwerkingenregister lastig voor corporaties. “De makkelijkste manier om dit te doen is door de verantwoordelijkheid voor het bijhouden lager in de lijn te leggen. Proceseigenaren zijn het beste op de hoogte van wijzigingen en kunnen sneller constateren wanneer de lijst bijgewerkt dient te worden door de privacy officer. Daarbij is het goed om ieder jaar of bij wijzigingen de lijst nog eens door te lopen, om te voorkomen dat over een paar jaar een verouderd register in z’n geheel bijgewerkt dient te worden.”

Tijdrovend

Waar negen op de tien corporaties bewaartermijnen heeft ingericht, verwijdert en vernietigt slechts 35 procent daadwerkelijk de data. Op de vraag waarom plannen worden gemaakt die niet worden nageleefd, zegt Suzanne: “Het maken van plannen is een belangrijke stap in het bewust omgaan met gegevens. Het is nu bij alle corporaties wel duidelijk dat er op informatie bewaartermijnen staan en deze nageleefd dienen te worden. Bewaartermijnen staan echter niet altijd hoog op de agenda; het is immers een erg tijdrovende klus en eentje die niet actief bijdraagt aan de doelen van een corporatie. Daarnaast is het verwijderen van data vaak ook het ‘loslaten’ van een gevoel van zekerheid en controle. Die stap nemen steeds meer corporaties, maar wel op het moment dat het voor hen goed voelt.”

Minimaliseren van data

Het eerdergenoemde dataminimalisatie is dan ook de volgende stap: “Dit is een mooi voorbeeld van ‘privacy by design’,” vertelt Suzanne. “Vraag en gebruik alleen de gegevens die je nodig hebt, tot je het doel bereikt hebt en gooi het daarna weg. Het verwerkingenregister geeft inzicht in welke gegevens verwerkt worden, en nu is het tijd om kritisch processen te doorlopen en te kijken met welk doel gegevens verzameld en verwerkt worden. Het minimaliseren van data kan daarbij helpen processen te optimaliseren.”

Controles en audits

Uit de steekproef blijkt ook dat controle (70 procent) en audits (60 procent) steeds vaker door corporaties worden uitgevoerd. “Deze zijn essentieel voor een werkende PDCA-cyclus. Zonder controle van je maatregelen kun je nooit weten of afspraken daadwerkelijk worden nageleefd. Met als gevolg dat je wellicht niet zo compliant bent als alle procedures en beleid doen vermoeden.”

Eigen podium

Suzanne trekt uit de steekproef een opvallende conclusie omtrent informatiebeveiliging. Omdat corporaties veel aandacht hebben geschonken aan de AVG, is dit volgens haar een ondergeschoven kindje geworden. “Informatiebeveiliging was voor velen ‘een artikel in de AVG’, waar passende beveiliging van persoonsgegevens als vereiste wordt gesteld. Ook werd dit vaak opgenomen in een AVG-plan van aanpak. Informatiebeveiliging is echter zoveel meer dan dat en verdient een eigen podium. Nu data zo essentieel zijn voor corporaties dat ze er veelal afhankelijk van zijn, vormt informatiebeveiliging een van de belangrijkste waarborgen van de continuïteit van de business. Hierbij gaat het niet alleen om het beveiligen van persoonsgegevens, maar het beveiligen van alle gegevens.”

Vanzelfsprekendheid

Ondanks alle stappen zijn er altijd nog corporaties die niet helemaal AVG-ready zijn. Volgens Suzanne is dat echter niet uniek aan de corporatiesector. “AVG-ready worden vraagt tijd, aandacht en prioritering van een organisatie. Ik verwacht dat wanneer wij over een jaar opnieuw een steekproef zouden houden, corporaties privacybewuster werken dan nu. Daarbij zou het mooi zijn als het steeds minder gaat over de AVG en het voldoen aan regels, maar dat privacybewust werken een vanzelfsprekendheid wordt voor alle organisaties.”

Deelname

Corporaties die meer willen weten over de onderzoeksresultaten over AVG compliance of willen bijdragen aan het onderzoek, kunnen contact opnemen met Audittrail. “We willen toe naar een zo breed gedragen mogelijke AVG benchmark in de sector.” ■