RIEN HOMMES VAN RSM RISK ADVISORY SERVICES OVER AANGESCHERPTE PRIVACYWET:

‘VERGEET MEI NIET’

IT-AUDITOR RIEN HOMMES LEIDT BINNEN RSM DE RISK ADVISORY SERVICES GROUP. DE LAATSTE MAANDEN IS ZIJN WERK-TERREIN – PRIVACYWETGEVING – ‘HOT’. DE NIEUWE EUROPESE WET, IN NEDERLAND BEKEND ALS DE ALGEMENE VERORDENING GEGEVENSBESCHERMING (AVG), TREEDT OP 25 MEI DEFINITIEF IN WERKING.

GWEN VAN LOON ERIK VAN DER BURGT

Alle bedrijven en instellingen die persoonlijke data opslaan, krijgen met de AVG te maken. ‘Juristen begrijpen precies hoe de verordening in elkaar steekt en hebben de juridische vertaalslag gemaakt. Wij helpen organisaties hun procedures aan te passen, zodat ze klaar zijn voor deze strengere regelgeving. Mijn mantra is daarom de laatste maanden: vergeet mei niet’, aldus Rien Hommes.

RSM trekt in dit traject op met partner Key2Control dat de software-ondersteuning levert. Het team is inmiddels uitgebreid tot veertien medewerkers. ‘Niet alleen onze klanten moeten zich houden aan de AVG, wij zelf ook. Ook daar blijkt dat de praktijk ingewikkelder is dan theorie, al heeft de projectgroep nu voor heel RSM in Nederland één uniforme set van procedures vast kunnen leggen.’

PITTIG

In de praktijk heeft Rien gezien dat veel partijen de aanpassingen in hun administratie aanvankelijk voor zich uit hadden geschoven. ‘Maar de deadline van 25 mei is keihard. Vanaf dat moment start de handhaving. Boetes kunnen oplopen tot 4% van de omzet, met een maximum van € 20 miljoen. Pittig natuurlijk. Ik verwacht dat de soep in de meeste gevallen niet zo heet wordt gegeten, want er is ook een arsenaal aan lagere boetes. Feit is dat het personeelsbestand van de privacywaakhond Autoriteit Personeelsgegevens (AP) voor eind dit jaar wordt uitgebreid van 100 naar 400 medewerkers om de handhaving, die tot nu toe nauwelijks plaatsvindt, waar te kunnen maken.’

Rien verwacht dat bepaalde sectoren als eerste onder het vergrootglas liggen: de gezondheidszorg en gemeentes die verantwoordelijk zijn voor het sociale domein. Datalekken moeten onverhoopt gemeld worden en wie vermoedt dat er verkeerd met zijn gegevens wordt omgegaan, kan dat melden bij de AP.

DATAMARKETING

Rien is blij dat de nieuwe wetgeving Europees is geregeld. ‘Eerst had elk land zijn eigen privacyverordening. Dat maakte het hartstikke lastig als je in meerdere landen actief was, helemaal als je deze gevoelige gegevens door derden liet verwerken, zoals bij payrolling en datamarketing gebeurt. Nu geldt in elk van de 28 lidstaten van de EU simpelweg dezelfde wetgeving. Dat maakt de zaak in elk geval duidelijker.’

Zo liggen alle processen waarbij een ID-bewijs om de hoek komt kijken onder het vergrootglas. ‘Want je mag de gegevens die daarop staan niet langer zo maar bewaren en in je administratie opnemen. Bovendien heeft iedereen volgens de AVG het ‘recht-om-vergeten-te-worden’. Degene die de data beheert, moet jouw gegevens per direct kunnen verwijderen. Niet alleen in zijn eigen administratie, maar ook in die van partijen waarmee een samenwerkingsverband bestaat. Ingewikkeld dus.’

EUROPESE PRIVACYWET

De Europese General Data Protection Regulation (GDPR) is in Nederland bekend als de Algemene verordening gegevensbescherming (AVG). Het is de opvolger van de Wet bescherming persoonsgegevens. Vanaf 25 mei wordt erop toegezien dat iedereen zich houdt aan de striktere regelgeving. Wie zich niet committeert aan de strengere eisen loopt het risico flink bestraft te worden.

RSM heeft de afgelopen jaren op tal van plekken nulmetingen gedaan en interviews om de bestaande situatie in kaart te brengen. Daarop volgde een GAP-analyse en vervolgens een implementatieplan, ondersteund door de software van Key2Control met wie RSM in dit traject samenwerkt. Vaak leidt het tot nieuwe contracten tussen de opdrachtgever en partijen met wie hij samenwerkt.

‘Degene die de privacygevoelige informatie verzamelt, blijft verantwoordelijk voor de gegevens. Ook als een samenwerkingspartner, de verwerker, de data zou opslaan of bewerken. Dat moet contractueel goed geregeld zijn, vandaar dat veel afspraken een aanpassing behoeven’, aldus Rien Hommes. Bijna alle bedrijven zijn verplicht een verwerkings- en een incidentenregister aan te leggen. ‘Wij adviseren om dat te bundelen in één register, samen met de grondslag waarop de verwerking van privacygegevens wordt uitgevoerd.’

De gegevens van mensen die overstappen van energieleverancier of telecomprovider mogen nog steeds worden overgedragen naar een nieuwe aanbieder om de overgang soepel te laten verlopen. ‘Maar daarna moeten ze jouw gegevens wissen. Ze mogen ze dus niet langer bewaren om je later over te halen terug te keren als klant.’

LEDENADMINISTRATIES

Ook in de gezondheidszorg, bij clubs met ledenadministraties (zoals charitatieve instellingen en sportclubs) en overheidsinstanties (gemeenten, provincies en Rijk) heeft de nieuwe wetgeving veel impact. ‘En dan heb je het nog niet over de mensen die je actief benaderen om hun data te vernietigen of vragen hen te laten zien met wie je hun gegevens hebt gedeeld. Bij de gemeente kun je je bijvoorbeeld beroepen op inzagerecht: aan wie zijn mijn gegevens doorgespeeld? Dat moet je kunnen overleggen als gemeente. Mijn collega’s en ik kregen verbaasde blikken toen we het uit gingen testen, al zijn er gemeenten die het proces al goed op de rit hebben staan.’

BSN-GEGEVENS

‘De eisen zijn echt heel streng. Ook werkgevers mogen niet zomaar privacygevoelige informatie opslaan. Zo is nauwkeurig omschreven van wie je zaken als NAW-gegevens (naam/adres/woonplaats, GvL) en bankrekeningnummers mag bewaren. En BSN-gegevens die we in Nederland gebruiken voor identificatie mogen niet langer gekoppeld worden aan marketingdoeleinden. Werkgevers mogen die alleen gebruiken voor de salarisverwerking, omdat die is gekoppeld aan een overheidstaak; het innen van belastingen. Nieuwe werknemers of klanten mag je voortaan alleen nog identificeren, maar een kopie maken van het complete paspoort is uit den boze. Heb je die wel in bezit, dan moet je die vernietigen.’

Ook partijen als Facebook, Google en LinkedIn draaien volgens Rien de laatste tijd flink overuren, omdat de oude manier waarop ze omgingen met data in het AVG-tijdperk niet meer mag. ‘Je moet iedereen in Europa expliciet opnieuw om toestemming vragen zijn gegevens te bewaren. En iedereen kan die elk moment weer intrekken.’ De strengere regels gelden in principe alleen voor EU-ingezetenen en voor organisaties die werken in de EU, ook als hun gegevens worden opgeslagen in de VS. De regels zijn dus strenger dan daar. ‘Maar je ziet dat die wereldwijdopererende bedrijven de AVG voortaan als uitgangspunt nemen.’

VOOR MEER INFORMATIE KUNT U CONTACT OPNEMEN MET RIEN HOMMES VAN RSM RISK ADVISORY SERVICES VIA RHOMMES@RSM-NL.NL