Column: Brink's Blik

Laat uw nachtrust niet verstoren door de GDPR

Amerikanen innoveren, Chinezen kopiëren en Europeanen reguleren. Deze stelling kwam ter sprake tijdens het Risk en Compliance Jaarcongres op 1 juni in Baarn. Ik kan hem grotendeels beamen. Zo gaat op dit moment veel aandacht uit naar de nieuwe dataprivacywetgeving in de Algemene Verordening Gegevensbescherming, beter bekend onder zijn Engelse naam General Data Protection Regulation (GDPR). Niet naleven van deze verordening kan flinke financiële consequenties hebben. Ruim de helft van de bedrijven in Nederland is echter nog niet serieus begonnen met de voorbereidingen. Bij veel organisaties is daarom geen sprake van zomerflauwte of adempauzes. Wel van stevig doorwerken om voor mei 2018 compliant te zijn.

De laatste jaren volgen de ontwikkelingen op het gebied van wet- en regelgeving in Europa (maar vlak Amerika niet uit) elkaar in hoog tempo op. De GDPR is in mei 2016 in werking getreden. Belangrijkste aanleiding was een aantal ingrijpende datalekken, zoals het telefoonboek van de HR afdeling van het Belgische leger en de data van 77 miljoen klanten in het Playstation Network. Het vervallen van het zogenaamde 'Safe Harbour akkoord' - dat het door Amerikaanse bedrijven voldoen aan Europese privacywetgeving regelde – is ook een belangrijke push in de richting van GDPR gebleken.

> In 2016 zijn in Nederland bijna 5500 datalekken gerapporteerd, klein en groot

Wist u dat er in 2016 bijna 5500 datalekken, klein en groot, aan de Autoriteit Persoonsgegevens zijn gerapporteerd? En dat 17% daarvan voortkwam uit de financiële sector? Dat zijn bijna 1000 incidenten in één jaar! Niettemin sprak ik laatst iemand die de aandacht voor dit onderwerp maar overdreven vond.
Mijn voorbeeld over het inzien van andermans rekeninggegevens in een klantportal deed hem gelukkig toch van mening veranderen.

Wat regelt de GDPR?
De GDPR dient ter 'bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en het betreffende vrije verkeer van die gegevens'. Hij vervangt de Europese databeschermingsrichtlijn uit 1995, die niet meer voldeed in het huidige digitale tijdperk.

Onder de GDPR is het opslaan van en omgaan met persoonlijke data behoorlijk aangescherpt. Van organisaties wordt verwacht dat zij voor mei 2018 handelen conform de GDPR. Niet voldoen aan de regelgeving (non-compliance) kan vergaande financiële gevolgen hebben. Iedereen – burgers, bedrijven, overheden - mag organisaties namelijk op naleving van de GDPR aanspreken. De maximale boete voor non-compliance is 20 miljoen euro of, in het geval van een onderneming, 4% van de jaarlijkse wereldwijde omzet, afhankelijk van welk bedrag hoger is. Genoeg reden om ruim tijd en aandacht te besteden aan de GDPR, lijkt mij.

> Het is zaak om zo snel mogelijk een GDPR impactanalyse te beginnen dan wel af te ronden

Waar gaat het om?
In vogelvlucht een paar elementen uit de GDPR:

- Europese burgers krijgen weer controle over hun persoonlijke data. Wie bewaart wat, hoe lang en op welke manier? De rechten van het zogenaamde 'data subject' zijn uitgebreid. Dit betreft bijvoorbeeld het recht tot doorhalen van gegevens, rectificatie alsmede het opvragen van informatie of er persoonlijke data wordt verwerkt, hoe dit gebeurt en waarom.
- Strenge regels met betrekking tot 'accountability'. Hoe toon je als dataverwerker aan dat je compliant bent met deze nieuwe wet?
- De definitie van persoonlijke data is opgerekt en betreft nu ook woonplaats, IP adres, Burger Service Nummer, Legal Entity Identifier, et cetera.
- De regels voor het vragen van toestemming voor het gebruik van data zijn aangescherpt. In zijn algemeenheid moet die toestemming veel explicieter aan de betrokkene worden gevraagd en moet de toestemming worden gearchiveerd.
- Datalekken moeten binnen 72 uur worden gerapporteerd aan de nationale 'Data Protection Authority'. In Nederland is dat de Autoriteit Persoonsgegevens, onderdeel van het Ministerie van Veiligheid en Justitie.
- Regels met betrekking tot data transfer buiten de Europese Unie of de Europese zone.
- De benoeming van een Data Protection Officer bij organisaties die onder de GDPR vallen. Het zal u niet verbazen dat aan deze functionaris allerlei eisen worden gesteld. Maar wees gerust, uw tennisvereniging hoeft voor de ledenadministratie geen Data Protection Officer aan te wijzen.

Begin tijdig met de invoering binnen uw organisatie
Bij KAS BANK houdt een speciale werkgroep 'Monitoring Future Trends and Regulations' zich bezig met nieuwe wet- en regelgeving, waaronder dus de GDPR.

Deze werkgroep bestaat o.a. uit collega's van Corporate Development, Client Management, Risk, Legal en Compliance. Onze eerste afdronk is dat wij, gezien de aard van onze dienstverlening, beperkt geraakt worden door de GPDR. Wij zijn immers een wholesale bank en slaan geen grote hoeveelheden data van individuen op. Dat wil overigens niet zeggen dat wij rustig achterover kunnen leunen.

Voor onze klanten, en dan vooral de pensioenfondsen en verzekeraars, is de impact van de GDPR veel groter. Zij verwerken en archiveren immers wel grote hoeveelheden persoonlijke gegevens. Gezien de korte implementatietijd van de GDPR (mei 2018) en het feit dat u waarschijnlijk al veel capaciteit inzet op MiFID II, is onze aanbeveling dan ook om zo spoedig mogelijk met een GDPR impactanalyse te beginnen dan wel deze analyse zo snel mogelijk af te ronden.

Gezonde nachtrust
Ondertussen houdt het niet op met nieuwe regelgeving. Na MiFID II (januari 2018) en GDPR (mei 2018) staat over anderhalf jaar alweer de Securities Financing Transactions Regulation (SFTR), oftewel de 'shadow banking regulation' voor de deur. Het merendeel van de nieuwe regelgeving heeft (gelukkig) een duidelijke functie. De praktische implementatie en uitvoering kost organisaties echter veel tijd. Net als het anticiperen op nieuwe wetgeving die wel al is aangekondigd, maar nog niet is uitgewerkt.

Mocht u over al deze ontwikkelingen met ons van gedachten willen wisselen, dan staan wij uiteraard tot uw beschikking. Eén advies wil ik u daarbij alvast meegeven. Als u van een goede nachtrust wilt blijven genieten, begin dan tijdig met de inventarisatie en implementatie van nieuwe regelgeving. Uit eigen ervaring kan ik zeggen dat dit de beste remedie is tegen slapeloosheid.