De Panama Papers – hoe nu verder?

Anja Dekhuijzen houdt zich als vooraanstaand advocaat bij Whitebridge bezig met IT- en outsourcing. Ze adviseert in die hoedanigheid cliënten over vraagstukken rondom outsourcing, IT-contracten, IT-disputen, telecommunicatie, e-commerce en privacy.

De Panama Papers zijn wereldwijd het grootste datalek ooit. Het betreft het topje van de ijsberg: door hackers zijn de data van 48 advocatenkantoren wereldwijd gehackt. De Panamese juridische en zakelijke dienstverlener Mossack Fonseca betreft slechts de eerste van deze 48 kantoren waarvan journalisten alle (persoons)gegevens op de computer hebben geordend in een bestand en op naam doorzoekbaar. In Nederland zijn *Het Financieele Dagblad* en *Trouw* erbij betrokken.

Maar niet alleen dergelijke geruchtmakende datalekken vinden plaats. Sinds 1 januari 2016 geldt in Nederland de wettelijke meldplicht datalekken. Een datalek is een inbreuk op de beveiliging van een organisatie, waarbij verlies van persoonsgegevens plaatsvindt. Denk bijvoorbeeld aan verlies van een laptop of USB-stick. Maar ook een hack of malware kan leiden tot een datalek.

Belangrijk bij outsourcing is dat veel datalekken zullen plaatsvinden bij de outsourcingsleverancier. Deze zal in de praktijk vaak degene zijn waar de persoonsgegevens zich op de server bevinden, en deze zal vaak de persoonsgegevens verwerken in opdracht van de outsourcende partij. Stel dat een datalek plaatsvindt bij uw outsourcingsleverancier, maar deze vertelt dit u niet. Wat velen zich niet realiseren is dat men (als outsourcende partij) zélf verantwoordelijk blijft voor een datalek en het melden ervan, ook als het datalek bij de bewerker plaatsvindt. Het is dan ook van cruciaal belang dat in de bewerkersovereenkomst met de outsourcingsleverancier afspraken worden gemaakt rond datalekken. Dit is bovendien per 1 januari 2016 wettelijk verplicht.

De boetes voor datalekken zijn niet mals. Deze zijn momenteel 820.000 euro of, als dit niet een passende boete zou zijn, 10 procent van de jaaromzet. In de recent aangenomen Europese Privacyverordening, die per 25 mei 2018 de Nederlandse Wet bescherming persoonsgegevens (Wbp) gaat vervangen, wordt deze boete substantieel verhoogd: naar 20 miljoen euro, of als dit niet een passende boete zou zijn, 4 procent van de jaaromzet. Het gaat telkens om het hoogste van de twee bedragen.

Het verplicht moeten melden van een serieus datalek leidt tot veel onrust bij organisaties. Bij het al dan niet opleggen van boetes door de Autoriteit Persoonsgegevens (AP) is onder meer van belang of men het achterliggende privacybeleid op orde heeft. Met andere woorden, of men rechtmatig of juist onrechtmatig persoonsgegevens verwerkt. In de praktijk is dit bij veel organisaties nog niet op orde, zodat het vooruitzicht van een boete helaas niet imaginair is.
Bovendien kan een dergelijke boete naar de letter van de wet tevens aan een bestuurder *in privé* worden opgelegd. Hierbij moet men denken aan twee situaties: namelijk de boete wordt opgelegd aan degenen die tot het datalek opdracht hebben gegeven, alsmede aan hen die feitelijk leiding hebben gegeven aan de verboden gedraging.

Niet ieder datalek moet worden gemeld (en derhalve tot boetes leiden): in de huidige Wet meldplicht datalekken, zoals opgenomen in de Wbp, moet een datalek worden gemeld als er een aanzienlijke kans is (of het zeker is) dat het datalek *ernstige* nadelige gevolgen heeft voor de bescherming van persoonsgegevens. Vanaf 25 mei 2018 wordt de meldplicht sterk verruimd: een datalek zal dan moeten worden gemeld aan de AP, tenzij het *onwaarschijnlijk* is dat het datalek zal resulteren in *een risico* voor de privacy van individuen. Aangezien alleen meldplichtige datalekken tot een boete kunnen leiden, wordt dus ook het boeteregime verruimd (en verhoogd tot voornoemde 20 miljoen euro).

Hoog tijd om uw privacybeleid en -beveiliging in lijn te brengen met de wet!