WWW.MINDYOURSTEP.INFO

Meldplicht Datalekken

wanneer en hoe moet ik een datalek melden aan de Autoriteit Persoonsgegevens?

De vraag

Sinds 1 januari 2016 hebben bedrijven, overheden en andere organisaties die persoonsgegevens verwerken de plicht om een melding te maken wanneer er zich een datalek heeft voorgedaan. Maar wanneer en hoe moet je een datalek melden? Lang niet alle datalekken hoeven namelijk gemeld te worden bij de Autoriteit Persoonsgegevens. Belangrijk dus om helder te hebben in welke situatie je als organisatie een datalek moet melden en hoe je dat moet doen.

De uitdaging

Een datalek moet volgens de wet gemeld worden aan de Autoriteit Persoonsgegevens als er sprake is van een ernstig datalek. Hierbij moet je denken aan het lekken van persoonsgegevens van gevoelige aard of wanneer de aard en de omvang van het lek kunnen leiden tot ernstige nadelige gevolgen. Maar let op, sinds de Algemene Verordening Gegevensbescherming van toepassing is, moet jouw organisatie alle datalekken documenteren. Op die manier kan de Autoriteit Persoonsgegevens controleren of jouw organisatie aan de meldplicht datalekken heeft voldaan.

Bij het beantwoorden van de vraag of er sprake is van (een aanzienlijke kans op) nadelige gevolgen voor de bescherming van persoonsgegevens moet je dus kijken naar de aard van de getroffen gegevens. Als de gelekte gegevens bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard zijn, dan kun je er redelijkerwijs vanuit gaan dat je het lek moet melden. Het gaat dan bijvoorbeeld om gegevens over iemands godsdienst, levensovertuiging, gezondheid, lidmaatschap van een vakvereniging, gegevens over de financiële of economische situatie, prestaties op school of werk, gebruikersnamen, wachtwoorden en andere inloggegevens of gegevens die kunnen worden misbruikt voor identiteitsfraude. Maar denk ook bijvoorbeeld aan het op straat komen te liggen van veel gegevens van één persoon, van gegevens van grote groepen betrokkenen of van gegevens van kwetsbare groepen. Deze gegevens zijn aantrekkelijk voor het criminele circuit en hebben een verhoogde kans om doorverkocht te worden, met als gevolg dat de betrokkenen langer last houden van het datalek.

De oplossing

Kortom, om te bepalen of je een datalek moet melden moet je jezelf twee vragen stellen:

1. Is er sprake van bijzondere persoonsgegevens of van persoonsgegevens die anderzijds van gevoelige aard zijn?
2. Leiden de aard en omvang van de inbreuk tot (een aanzienlijke kans op) ernstige nadelige gevolgen?

Wanneer je één of beide vragen bevestigend beantwoord is de meldplicht van kracht. Het lek moet je vervolgens binnen 72 uur na de ontdekking aan de Autoriteit Persoonsgegevens melden.

Dat kun je doen via het door de Autoriteit Persoonsgegevens beschikbaar gestelde webformulier op datalekken.autoriteitpersoonsgegevens.nl.

Na het invullen van het webformulier, krijg je een meldingsnummer te zien ter bevestiging. Noteer dit nummer voor verdere communicatie met de Autoriteit Persoonsgegevens.

Vergeet niet de betrokkenen, wiens data is gelekt, in een geval van een datalek te informeren indien er waarschijnlijk sprake is van een hoog risico voor de rechten en vrijheden van de betrokkenen.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak.
Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.