(Vermoedelijk) datalek melden

Datalek melden

Vanaf 1 januari 2016 is de meldplicht Datalekken van kracht. Dit houdt in dat bedrijven en organisaties die persoonsgegevens van patiënten, medewerkers of ketenpartners verwerken, verplicht zijn om (potentiële) datalekken te melden aan de toezichthouder, de Autoriteit Persoonsgegevens. In bepaalde gevallen moet dit ook gemeld worden aan de betrokkene van wie de gegevens zijn gelekt. Als blijkt dat niet of onvoldoende is voldaan aan deze meldplicht kan de toezichthouder een boete opleggen.

ER MOET IN IEDER GEVAL GEMELD WORDEN ALS:

Zijn gegevens (definitief) verloren gegaan?	→	ja	→	melden
Zijn de gegevens bijzonder of zeer omvangrijk?	→	ja	→	melden
Zijn de gegevens in onbevoegde handen geraakt?	→	ja	→	melden
Aanzienlijk risico op schade aan persoonlijke levenssfeer?	→	ja	→	melden
	→	Nee op alle vragen	→	niet melden

WAT IS EEN DATALEK?

Volgens de AVG is er sprake van een datalek als per ongeluk, opzettelijk of onrechtmatig persoonsgegevens vernietigd, verloren of gewijzigd worden, of als ongeautoriseerde openbaring van die gegevens plaatsvindt. Voorbeelden van een datalek zijn het verlies van een mobiel apparaat waarop gevoelige persoonsgegevens staan. Maar ook computer hacking, stroomuitval (waardoor gegevens verloren gaan) of inzage van privé gegevens door een onbevoegd persoon. Dit kan gebeuren doordat je bijvoorbeeld informatie per mail verstuurt aan een mailadres waarvan je niet zeker weet of dit ook bij de persoon in kwestie hoort. Ook als een receptioniste gegevens over een betrokkene niet afschermt (bijvoorbeeld in een telefoongesprek) waardoor een andere cliënt dingen hoort die herleidbaar zijn tot een privépersoon, dan is dat een datalek.

MELDEN BIJ DE AUTORITEIT PERSOONSGEGEVENS

Niet ieder datalek-incident valt onder de meldplicht. Als bijvoorbeeld verloren of gestolen persoonsgegevens goed versleuteld zijn opgeslagen, dan is er geen aanzienlijk risico op schade aan de persoonlijke levenssfeer. Maar als bijvoorbeeld zonder toestemming van een betrokkene bekend wordt dat hij patiënt of cliënt bij een zorgorganisatie is, dan wordt dat als schadelijke inbreuk op de privacy beschouwd.

Een datalek dient uiterlijk *binnen 72 uur* na ontdekking te worden gemeld aan de toezichthouder. Deze melding wordt verzorgd door de Functionaris Gegevensbescherming (FG). Bovendien moet gemeld worden hoe het lek heeft kunnen plaatsvinden en wat er gedaan wordt om het lek te dichten. Het kan immers zijn dat een werkproces foutgevoelig is en voor verbetering vatbaar is. Daarom zal de FG bij een datalek altijd een analyse maken van de situatie en betrokkenen helpen met suggesties om herhaling te voorkomen.

Proces melden (vermoedelijk)datalek