HELP, een *datalek!*

Tuurlijk beveiligt u uw pc's goed. En uw laptop wordt ook niet gestolen. Maar hoe verantwoord gaan uw mensen om met een USB-stick of wachtwoord? En downloaden ze nooit eens software met een hackvirusje...? Voor u het weet liggen persoonsgegevens op straat. U loopt daarbij nu kans op een fikse boete.

TEKST | LOES GROOTERS FOTOGRAFIE | ANDREA LOOT

Eerste hulp bij datalekken – zo viel het IKT College op 16 februari ook wel te noemen. Bij Van der Valk Hotel Hengelo deelde Mirjam Elferink haar tips en ervaringen op dit vlak. De advocaat van KienhuisHoving verdiept zich al jaren in intellectuele eigendom, ICT-recht en privacy. Met die thema's is ze sinds 1 januari 2016 extra druk. Want toen ging de nieuwe Wet meldplicht datalekken in. Die 'belooft' 810.000 euro boete aan organisaties die persoonsgegevens lekken.

Camerabeeld als persoonsgegevens?

Volgens de wet gaat het bij persoonsgegevens om alle informatie over een individu. Zelfs als dat individu anoniem is, zoals in de ritadministratie van taxibedrijven. Want met routegegevens kunnen individuele chauffeurs worden opgespoord. En of u nu persoonsgegevens bijhoudt op papier, in de computer, op camerabeelden of via stemopnamen - ze vallen allemaal onder de nieuwe wet.

Maar ik kon er niets aan doen...

Lekt uw bedrijf persoonsgegevens? Dan maakt de overheid geen verschil in de oorzaak: per ongeluk, overmacht (diefstal), bewust. Een van de grootste risico's voor al deze datalekken is de mens En dus raadt Elferink bedrijven aan medewerkers bewust te maken van de gevaren en gevolgen hiervan. En toe te zien op het voorkomen van lekken, bijvoorbeeld door hun mail te controleren. Maar of dat altijd zo maar mag...? Het is volgens haar inderdaad zoeken naar balans tussen beschermen van medewerkersprivacy én de plicht om de persoonsgegevens van derden te beschermen. De tips uit het kader helpen hierbij, net als bij verkleinen van de kans op 'datalekkage'.

Mirjam Elferink
Advocaat bij KienhuisHoving

Op weg naar datalek-proof **vier tips**

1. Monitor werknemers
Check bijvoorbeeld hun internet- en mailgebruik op uw pc's em mobiele telefoons. Addertje: Dit mag alleen met een geldig doel. Stel daarom eerst regels op over gebruik van uw bedrijfsmiddelen (ICT-protocol).

2. Pas de overeenkomst met bewerkers aan
Verwerkt een externe partij persoonsgegevens voor u? U bent verplicht een bewerkersovereenkomst te sluiten. Zet hierin dat hij de gegevens alleen in opdracht van u mag verwerken, en volgens uw instructies. Vermeld ook dat hij de boel goed moet beveiligen en een datalek aan u móet melden.

3. Stel een datalekprotocol op:
Bedenk daarbij vooraf mogelijke scenario's bij datalekken. Zet daarbij op papier wat u doet om schade te beperken. Vermeld ook dat u de volgende punten moet doorgeven aan de Autoriteit Persoonsgegevens (AP):
A- aard van de inbreuk;
B- de instanties waar meer informatie over de inbreuk is te krijgen;
C- de adviesmaatregelen om de negatieve gevolgen van de inbreuk te beperken (zoals: veranderen van gebruikersnamen en wachtwoorden);
D- beschrijving van de ontdekte en vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
E- de maatregelen die uw organisatie neemt/voorstelt om deze gevolgen te verhelpen.

4. Houd een lijst van inbreuken bij
De wet verplicht u dit. Zet erbij welke gegevens u aan de AP doorgaf. En wat u de mensen liet weten van wie u de gegevens lekte.