**Stappenplan in geval van Datalek**

Praktijk Mesologie Groningen

In het geval de Praktijk Mesologie Groningen onverhoopt te maken krijgt met een datalek, dan volgt de Praktijk Mesologie Groningen het door de Autoriteit Persoonsgegevens gehanteerde stappenplan. Dit plan behelst vijf (5) stappen die te nemen zijn.

1. Praktijkhoudster is de verantwoordelijke persoon te handelen in geval van een datalek
2. Praktijkhoudster analyseert zo snel mogelijk de situatie (***overzicht***). Wat is er gebeurd en wat is de omvang van het lek? Gaat het om een inbreuk door gelekte, vernietigde of gewijzigde gegevens? Als gegevens zijn gelekt, onderzoekt praktijkhoudster wie er (mogelijk) toegang hebben (gehad) tot welke persoonsgegevens. Op deze informatie moeten de vervolgstappen worden gebaseerd.
3. De **schade** wordt zo snel mogelijk **beperkt**. Op basis van stap 1 wordt bepaald of er maatregelen zijn die meteen genomen kunnen worden het datalek te beëindigen en de schade te beperken. Zo ja, neemt praktijkhoudster deze maatregelen onmiddellijk. Zij maakt tegelijkertijd een inschatting van het (mogelijke) risico dat het datalek oplevert.
4. De praktijkhoudster gaat na of het lek wel of niet **gemeld moet worden bij de AP**. Indien dit het geval is, zorgt praktijkhoudster ervoor dat dit binnen 72 uur nadat het lek is ontdekt, gedaan wordt. Een datalek melden bij de AP is verplicht, tenzij het niet waarschijnlijk is dat het datalek een risico oplevert voor de rechten en vrijheden van de betrokken personen.
5. Praktijkhoudster registreert het datalek in het verplichte datalekregister, ook wanneer het datalek niet gemeld wordt aan de AP.
6. Praktijkhoudster volbrengt een evaluatie van de gebeurtenis ten einde herhaling van een dergelijk voorval te voorkomen.