9. Kennisgeving in geval van een datalek

Wat te doen in geval van een datalek?

> *Een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.*
>
> Artikel 4.12 van de Algemene Verordening Gegevensbescherming

De Algemene Verordening Gegevensbescherming (AVG) eist van de verwerkingsverantwoordelijke en van de verwerker dat ze waakzaam zijn wat betreft de beveiliging van de verwerking van persoonsgegevens. En dit door geschikte beveiligingsmaatregelen te treffen om welke vorm van inbreuk op gegevens dan ook te voorkomen.

➡ **Een inbreuk in verband met gegevens is met andere woorden het verlies, de diefstal, de verstrekking of de vernietiging van persoonsgegevens, op opzettelijke of onopzettelijke wijze, maar ook de onbeschikbaarheid van de gegevens.**

Wat moet er worden gedaan in geval van inbreuk in verband met persoonsgegevens?

De praktiserende arts moet het incident vermelden in zijn register van incidenten. Het register van incidenten is een document dat alle incidenten bevat die verband houden met de verwerkingen.

Als de inbreuk op persoonsgegevens een risico inhoudt voor de persoonlijke levenssfeer van de patiënt (diefstal van niet-vercijferde laptop, hacking), is de praktiserende arts gehouden tot het melden van de inbreuk bij de Gegevensbeschermingsautoriteit (GBA), binnen een termijn van 72 kalenderuren vanaf de kennisneming ervan via het op de volgende website beschikbare formulier: **Melding van gegevenslekken | Gegevensbeschermingsautoriteit (gegevensbeschermingsautoriteit.be)**. Na 72 kalenderuren moet de reden van de vertraging worden aangevoerd.

Wanneer de inbreuk een hoog risico inhoudt op inbreuk op de persoonlijke levenssfeer van de patiënt, dient de inbreuk eveneens aan de patiënt te worden gemeld, behalve bij door de AVG bepaalde uitzonderingen*.

Risico voor de patiënt?

Afwezigheid van risico	Risico	Hoog risico
Er is sprake van een technisch hiaat (netwerkstoring, stroomstoring of een op tijd gestopte hacking, ...) En dit houdt geen schending van de persoonlijke levenssfeer van de patiënt in **Vermelding van het technische incident in het register van incidenten.**	Er is sprake geweest van inbreuk op gegevens (diefstal van niet-vercijferde laptop, hacking, ...) En het **risico bestaat dat dit de persoonlijke levenssfeer van de patiënt schendt** **Melding bij de GBA binnen de 72 uur + Vermelding in het register van incidenten.**	Er is sprake geweest van inbreuk op gegevens En dit **houdt een hoog risico op schending van de persoonlijke levenssfeer van de patiënt in** 1. Melding bij de GBA binnen de 72 uur 2. Mededeling aan de betrokken patiënt(en)* 3. Vermelding in het register van incidenten.

*Artikel 34.3 van de AVG

Concreet gezien

Beveilig de gegevens van uw patiëntenbestand maximaal om elk risico op inbreuk in verband met gegevens te vermijden

Neem in de onderaannemingsovereenkomsten met uw verwerkers de verplichting op van beveiliging ten laste van de verwerker, met inbegrip van een kennisgevingsplicht aan de verwerkingsverantwoordelijke binnen een vastgestelde termijn (bijvoorbeeld 24 uur vanaf de kennisneming)

Houd een register van incidenten bij van alle inbreuken in verband met persoonsgegevens

Evalueer het risico

Maak in geval van risico op inbreuk op de persoonlijke levenssfeer van de patiënt binnen max. 72 uur vanaf de kennisneming van de inbreuk melding bij de GBA

Breng de patiënt op de hoogte van deze inbreuk in geval van hoog risico op inbreuk op zijn persoonlijke levenssfeer