

## Beleid bij data veiligheidsincidenten (datalek)

Een datalek (of: data incident) is voor *Verloskundige Praktijk Een Goed Begin*: iedere inbreuk op de dataveiligheid die per ongeluk of op onrechtmatige wijze leidt tot:

- vernietiging van data of informatie,
- verlies van persoonsgegevens,
- wijziging van persoonsgegevens,
- ongeoorloofde verstrekking van persoonsgegevens,
- ongeoorloofde toegang tot opgeslagen persoonsgegevens,
- ongeoorloofde toegang tot doorgezonden persoonsgegevens.

Een datalek ontstaat onder andere als *Verloskundige Praktijk Een Goed Begin* het slachtoffer wordt van ransomware of een andere vorm van kwaadwillige hacking.

In het geval dat zich een dataveiligheids incident voordoet of een zwakte in de databeveiliging geconstateerd wordt door een medewerker, meldt hij dit zo spoedig mogelijk bij zijn of haar leidinggevende en de verantwoordelijke voor databeveiliging van *Verloskundige Praktijk Een Goed Begin*.

Na een incident analyseert *Verloskundige Praktijk Een Goed Begin* de oorzaak, de aanpak en de mogelijkheden om een dergelijk incident te voorkomen. Zij legt haar bevindingen vast in het formulier 'dataveiligheidsincident'. De maatregelen *ter voorkoming* van het incident worden na invoering geëvalueerd.

## Procedure bij een incident (datalek)

Wanneer er sprake is van een incident, volgt *Verloskundige Praktijk Een Goed Begin* de volgen procedure:

- *Verloskundige Praktijk Een Goed Begin* heeft een interne medewerker als Functionaris Gegevensbescherming (FG), nl Jacolien Rijdsdijk. Waveland ondersteunt deze interne FG juridisch en praktisch.
- Stel de interne FG direct op de hoogte van het incident.
- Betrek de interne FG bij alle verdere acties rond het incident
- intern meldingsformulier (zie onder aan deze pagina) invullen en opslaan in het dataveiligheids portaal.
- melder, leidinggevende en verantwoordelijke voor informatiebeveiliging/FG stellen vast welke actie genomen dient te worden op basis van het soort informatie, de hoeveelheid informatie en welke belanghebbenden door dit incident geraakt zouden kunnen worden.
- actie toewijzen aan uitvoerder(s).

### Wel of niet melden van het incident bij de autoriteit persoonsgegevens?

- *Verloskundige Praktijk Een Goed Begin* beoordeelt het incident door zich (intern) de volgende vraag te stellen:

**Levert het data incident risico op voor de aantasting van de rechten en vrijheden van cliënten?**

(Als aangetoond kan worden dat het datalek **geen** gevolgen heeft voor de rechten en vrijheden van cliënten, doet **Verloeskundige Praktijk Een Goed Begin** geen melding bij de Autoriteit Persoonsgegevens.)

Als het antwoord **NEE** is, meldt **Verloeskundige Praktijk Een Goed Begin** het incident niet bij de Autoriteit Persoonsgegevens, en vult **Verloeskundige Praktijk Een Goed Begin WEL** het interne formulier 'dataveiligheidsincident' in en slaat dit op dossier.

Als het antwoord **JA** is meldt **Verloeskundige Praktijk Een Goed Begin** het incident binnen 72 uur bij de Autoriteit Persoonsgegevens --> Meldingsformulier datalek. Klik hier --> **Autoriteit Persoonsgegevens**.

- dataverantwoordelijke/FG meldt aan de betrokken cliënten het incident, de maatregelen die genomen worden. **Verloeskundige Praktijk Een Goed Begin** meldt het incident alleen aan betrokkene indien na de genomen maatregelen toch nog een risico bestaat voor de rechten en vrijheden van de betrokkene of betrokkenen. Let op: een melding kan ook vereist zijn op basis van de Wkkgz.
- verantwoordelijke voor dataveiligheid/FG documenteert het incident, de actie en de correctieve maatregel(-en) en publiceert deze aan de betrokkenen binnen de organisatie.
- **Verloeskundige Praktijk Een Goed Begin** trekt lering uit het incident en stelt maatregelen vast ter voorkoming van een dergelijk incident.