MELDPROCEDURE INCIDENTEN EN DATALEKKEN

Versie: 1.0 · **Datum:** 6 november 2026 · **Classificatie:** Openbaar (publicatieversie)

Vivia verwerkt voor zorgorganisaties gezondheidsgegevens van hun cliënten en patiënten, onder meer via Vivia-Connect en de STIP-App. Wij nemen elk beveiligingsincident en elk datalek serieus. Op deze pagina leest u wat u bij ons kunt melden, hoe u dat doet en wat wij daarna doen.

Wat kunt u melden?

- **Een beveiligingsincident:** een gebeurtenis die de beschikbaarheid, juistheid of vertrouwelijkheid van onze diensten of van de gegevens daarin bedreigt. Denk aan verdachte toegang tot een account, een virus, een verkeerd verzonden bericht of een verloren laptop.
- **Een datalek:** persoonsgegevens zijn verloren gegaan, gewijzigd of in verkeerde handen gekomen, of iemand kon er zonder toestemming bij (AVG art. 4 lid 12).
- **Een vermoeden.** U hoeft niet zeker te weten dat er iets mis is. Meld liever te vroeg dan te laat.

Hoe meldt u?

Vivia heeft één meldpunt voor incidenten en datalekken:

- **Meldformulier:** www.vivia.nl/veiligheidsincident
- **Telefoon:** 085 773 2042

Bij een ernstig incident, zoals een vermoeden van ransomware of een datalek met gezondheidsgegevens, belt u het liefst. Zorgklanten met een 24/7-afspraak gebruiken hun calamiteitennummer.

Zet in uw melding geen namen, BSN's of medische gegevens van cliënten. Beschrijf wat er is gebeurd, wanneer u het merkte, welke dienst het betreft en welke organisatie het raakt. Wij nemen daarna contact met u op.

Wat doen wij met uw melding?

1. **Registreren.** Wij leggen uw melding vast en u krijgt een registratienummer.
2. **Beoordelen.** Wij bepalen hoe ernstig het incident is, welke diensten en zorgklanten zijn geraakt en of het om persoonsgegevens gaat. Ernstige incidenten pakken wij direct op, ook buiten kantooruren. Buiten kantooruren hangt de responstijd af van de afspraken in uw overeenkomst.
3. **Beperken en oplossen.** Wij nemen maatregelen om de schade te beperken en stellen bewijs veilig.
4. **Informeren.** Wij informeren de betrokken partijen, zoals hieronder beschreven.

5. **Leren.** Na een ernstig incident of datalek onderzoeken wij de oorzaak en verbeteren wij onze maatregelen. Daarbij gaat het om het verbeteren van de beveiliging, niet om het zoeken van een schuldige.

Wie informeert wie?

- **Gegevens van zorgorganisaties.** Voor Vivia-Connect, de STIP-App en onze privacy- en beveiligingsdiensten zijn wij verwerker en is de zorgorganisatie verantwoordelijk voor de gegevens. Bij een (mogelijk) datalek informeren wij de zorgorganisatie onmiddellijk, uiterlijk binnen 24 uur. De zorgorganisatie beslist zelf over een melding aan de Autoriteit Persoonsgegevens en informeert zelf haar cliënten. Wij helpen daarbij met feiten, aantallen en de genomen maatregelen.
- **Gegevens van Vivia zelf.** Het gaat dan bijvoorbeeld om gegevens van medewerkers, sollicitanten, websitebezoekers en contactpersonen. Bij een datalek met deze gegevens melden wij dat zelf binnen 72 uur aan de Autoriteit Persoonsgegevens als dat verplicht is. Bij een hoog risico informeren wij u ook rechtstreeks.

Wij geven geen informatie over een incident met gegevens van een zorgorganisatie aan derden, zoals de pers, zonder afspraak met die zorgorganisatie, tenzij de wet ons daartoe verplicht.

Kwetsbaarheid gevonden?

Heeft u een zwakke plek in onze systemen ontdekt? Meld die dan vertrouwelijk via ons meldformulier (kies "Kwetsbaarheid"). Lees eerst ons beleid voor het melden van kwetsbaarheden. Onderzoek de kwetsbaarheid niet verder dan nodig en deel haar niet met anderen voordat wij haar hebben opgelost.

Kwaliteit en toezicht

Deze procedure maakt deel uit van ons managementsysteem voor informatiebeveiliging volgens NEN 7510 en ISO/IEC 27001. Wij beoordelen de procedure elk jaar en na elk ernstig incident.