



JURIDISCH DOCUMENT

Incidentprocedure

Beveiligingsincidenten en datalekken

Definitief Versie 4 oktober 2026

1. Doel

Deze procedure beschrijft hoe Regivaro omgaat met (vermoedelijke) beveiligingsincidenten en datalekken, van signalering tot melding aan getroffen klantorganisaties.

2. Wat is een incident?

Een incident is elke gebeurtenis die de vertrouwelijkheid, integriteit of beschikbaarheid van gegevens binnen Regivaro in gevaar brengt of kan brengen, waaronder:

- Onbevoegde toegang tot gegevens van een organisatie
- Verlies of ongewenste vernietiging van gegevens
- Een kwetsbaarheid die misbruikt is of misbruikt had kunnen worden
- Verdachte inlogpogingen of gedrag dat op een aanval wijst

3. Stappen bij een (vermoedelijk) incident

1. Signaleren: iedereen (medewerker of gebruiker) die een vermoedelijk incident opmerkt, meldt dit direct, ongeacht tijdstip.
2. Vastleggen: tijdstip, omvang en eerste indruk van het incident worden direct genoteerd, voordat context verloren gaat.
3. Indammen: waar mogelijk wordt de oorzaak direct geïsoleerd — bijvoorbeeld door een lek te dichten, een sleutel in te trekken, of toegang te blokkeren.
4. Beoordelen: binnen 24 uur wordt vastgesteld of het een datalek betreft (d.w.z. of persoonsgegevens zijn geraakt), en wat de omvang is: welke organisatie(s), welke gegevens, hoeveel betrokkenen.
5. Melden aan getroffen organisatie(s): Regivaro informeert de getroffen klantorganisatie(s) onverwijld na de interne beoordeling, en in elk geval uiterlijk binnen 48 uur na de feitelijke ontdekking van het incident, met: aard van het incident, geraakte gegevens, genomen maatregelen, en vervolgstappen.
6. Herstellen: de kwetsbaarheid of oorzaak wordt structureel verholpen, niet alleen het directe symptoom.
7. Evalueren: binnen twee weken na afhandeling wordt het incident geëvalueerd — wat ging er mis, wat is er verbeterd, en zijn er structurele maatregelen nodig.

4. Verantwoordelijkheid voor melding bij de Autoriteit Persoonsgegevens

Regivaro treedt op als verwerker. De verwerkingsverantwoordelijke (de klantorganisatie) is zelf verantwoordelijk voor het beoordelen of een datalek gemeld moet worden bij de Autoriteit Persoonsgegevens en/of betrokkenen. Regivaro levert hiervoor alle relevante informatie aan binnen de in artikel 3 genoemde termijn.

5. Contact bij een incident

Vermoed je een beveiligingsincident? Neem direct contact op via **security@regivaro.nl**. Vermeld: wat je hebt gezien, wanneer, en (indien bekend) welke organisatie(s) het betreft.

6. Herziening

Deze procedure wordt periodiek herzien, en in ieder geval na elk incident waarbij ervaring is opgedaan die tot aanpassing aanleiding geeft.