

## Procedure hoe te handelen bij een (vermoedelijk) datalek

Deze procedure is opgesteld om duidelijkheid te verschaffen over het onderwerp datalekken, communiceer deze procedure ook met uw medewerkers! Het is goed om eerst wat achtergrondinformatie helder te krijgen. Wanneer spreken we over het lekken van data? Hoe gaan wij binnen de zorggroep hiermee om? Dit document geeft antwoorden op deze vragen.

### **Wat is een datalek?**

Zoals opgenomen in de Algemene Verordening Gegevensbescherming (artikel 4 punt 12) is er sprake van een datalek: *"bij 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 persoonsgegevens."*

Voorbeelden van datalekken zijn:

- het verlies van een USB-stick met niet-versleutelde persoonsgegevens;
- een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn geworden.

### **Interne procedure**

De zorggroep Gelders Rivierenland heeft een procedure opgesteld voor het melden van datalekken, deze wordt in bijlage 1 schematisch weergegeven in een flowchart. Indien er een beveiligingslek of incident wordt geïdentificeerd door medewerkers of door een verwerker – bijvoorbeeld in apparatuur of programmatuur – dient hiervoor een melding gemaakt te worden bij de beleidsmedewerkers. Het maken van een melding zal altijd eerst telefonisch geschieden via 0344-645802, vervolgens wordt van de melder verwacht de melding tevens per mail te versturen aan: [secretariaat@gezondrivierenland.nl](mailto:secretariaat@gezondrivierenland.nl). De beleidsmedewerkers leggen de melding vast in een register en beoordelen de melding gezamenlijk met de Functionaris Gegevensbescherming. Wanneer er geen sprake is van een datalek, zullen de beleidsmedewerkers de melding in het register bijwerken en de melder op de hoogte stellen van het besluit. Wanneer er wel sprake is van een datalek, zal de Functionaris Gegevensbescherming meedenken over de te ondernemen stappen. Vervolgens werken de beleidsmedewerkers de melding in het register bij en zetten de melding door naar het Dagelijks Bestuur.

Het Dagelijks Bestuur bespreekt de melding en neemt het besluit welke vervolgactie te ondernemen. Indien er vastgesteld is dat persoonsgegevens verloren zijn gegaan of dat onrechtmatige verwerking redelijkerwijs niet uit te sluiten valt, zal het Dagelijks Bestuur besluiten een melding te maken bij de Autoriteit Persoonsgegevens. Het genomen besluit wordt gecommuniceerd met de beleidsmedewerkers die vervolgens het register bij kunnen werken en de melder vervolgens informeren over het besluit omtrent de melding. De melding zal gedaan worden via:

<https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0>.

Klik op "Nieuwe Melding" en vul vervolgens de gevraagde informatie in. Tevens zal de betrokkene(n) - waarvan gegevens verloren zijn gegaan of van wie gegevens onrechtmatig verwerkt kunnen worden – geïnformeerd moeten worden over het voorval.

Leg een rapportage vast omtrent de melding, benoem daarin alle ondernomen stappen. Vanaf het moment van binnenkomst tot aan het maken van een melding bij de betrokkene(n). Zo is het voor de gehele organisatie duidelijk wie wanneer en met welke

reden actie heeft ondernomen. De Autoriteit Persoonsgegevens kan een verzoek doen om dit in te zien.

Indien bij een verwerker een dergelijk beveiligingslek of incident is geconstateerd, probeer dan zoveel mogelijk relevante informatie te verkrijgen. De maximale doorlooptijd vanaf constatering tot het maken van een melding mag volgens de richtlijnen van het AP 72 uur zijn.

## **Procedure voor medewerkers of verwerkers**

### **Wat te doen bij een (vermoedelijk) datalek?**

We spreken van een **datalek** als: persoonsgegevens kwijt zijn geraakt of wanneer het niet uit te sluiten valt dat persoonsgegevens onrechtmatig verwerkt kunnen worden.

Enkele voorbeelden:

- het verlies van een USB-stick met niet-versleutelde persoonsgegevens;
- een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- een besmetting met ransomware waarbij persoonsgegevens ontoegankelijk zijn geworden

### **Hoe te handelen?**

**Stap 1:** Bel de beleidsmedewerkers via het nummer 0344-645802.

**Stap 2:** Leg de situatie uit. Probeer zoveel mogelijk informatie te delen.

**Stap 3:** Maak een melding per (beveiligde) mail, deze melding versturen aan [secretariaat@gezondrijverland.nl](mailto:secretariaat@gezondrijverland.nl)

Je melding wordt intern behandeld, hierover mag je terugkoppeling verwachten.

# Bijlage 1. Flowchart



## Procedure datalekken

