

## Bijlage 5: DATALEKKEN

### 1. Wet meldplicht datalekken.

Als onderwijsorganisatie hebben we vanaf 1 januari 2016 de plicht datalekken te melden. Dit conform het gestelde in de Wet Meldplicht datalekken die per genoemde datum in werking is getreden.

Deze meldplicht houdt in dat wij onverwijld een melding moeten doen bij de Autoriteit Persoonsgegevens zodra wij een ernstig data lek hebben. En in een aantal gevallen moeten wij het data lek ook melden aan de betrokkenen (de mensen van wie de persoonsgegevens zijn gelekt).

### 2. Definitie

In ons privacyreglement is een omschrijving gegeven van een data lek: toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens) zonder dat dit de bedoeling is van onze organisatie.

(NB: Onder een data lek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens).

Als alleen sprake is van een zwakke plek in de beveiliging, spreken we van een beveiligingslek en niet van een data lek. Er hoeft dan geen melding gedaan te worden aan de Autoriteit Persoonsgegevens.

### 3. Wanneer melden?

Niet ieder data lek hoeft gemeld te worden aan de Autoriteit Persoonsgegevens. Onder punt 2 is hier al iets over gezegd.

Volgens de wet moet een melding gedaan worden aan de Autoriteit Persoonsgegevens als het data lek leidt tot een aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, of als het ernstige nadelige gevolgen heeft voor de bescherming van persoonsgegevens.

De meldplicht is alleen van toepassing op datalekken die plaatsvinden in geautomatiseerde gegevensbestanden waarvoor we als Stichting/scholen verantwoordelijk zijn (bijv. een Excel sheet met NAW-gegevens van klas 3a, de database met personeelsgegevens).

Bij de beslissing of we een gebeurtenis die zich heeft voorgedaan moeten melden aan de Autoriteit Persoonsgegevens, en eventueel daarnaast ook aan de betrokkene, moeten we een aantal afwegingen maken. Het onderstaande schema geeft deze afwegingen weer.



Een melding dient zonder onnodige vertraging en zo mogelijk niet later dan 72 uur na de ontdekking van het data lek te worden gedaan. Op de website van de Autoriteit Persoonsgegevens is voor dit doel een webformulier beschikbaar.

4. Een data lek is bij een leverancier.

Als scholen hebben we te maken met 'bewerkers': leveranciers die in opdracht van onze scholen persoonsgegevens opslaan, verwerken of verzamelen. Indien zich bij een van de bewerkers (leveranciers) een data lek voordoet dienen er ook een melding te doen van het lek.

5. Intern melden.

Indien zich binnen onze organisatie een (aanwijzing tot) data lek voordoet wordt dit door degene die het lek constateert onmiddellijk gemeld bij een van de leden van het College van Bestuur.

Het College van Bestuur maakt op basis van verkregen informatie de afweging geschetst bij punt 3, en zet de melding bij de Autoriteit Persoonsgegevens in gang.

Voor achtergrond informatie over de beveiliging van persoonsgegevens en over de meldplicht voor datalekken verwijzen we naar de website van de Autoriteit Persoonsgegevens.