Datalekprotocol [naam organisatie]
Versie [jaartal of nummer]

Een datalek kan verstrekkende gevolgen hebben. Het kan namelijk betekenen dat gevoelige of vertrouwelijke informatie algemeen bekend wordt of dat de concurrent er met bedrijfsinformatie vandoor gaat. Het is belangrijk dat bij het vermoeden of vaststellen van een datalek adequaat wordt gehandeld. Daarvoor is dit datalekprotocol opgesteld.

A. Beveiligingsincident of datalek

[redacted]

Kort gezegd wordt er gesproken van een datalek zodra persoonsgegevens door onbevoegden zijn verwerkt (hieronder hoort ook het slechts inzien van gegevens) of wanneer je niet met zekerheid kunt uitsluiten dat dit is gebeurd.

Het blijft bij een incident indien:

- Een USB-stick of laptop wordt gestolen of verloren, maar toegang tot dit apparaat door onbevoegden is onmogelijk of er kunnen geen persoonsgegevens worden geraadpleegd, bijvoorbeeld doordat deze niet lokaal zijn opgeslagen;

[redacted]

Een incident of datalek kan ontstaan door:

- Moedwillig handelen, bijvoorbeeld een hack;
- verlies van gegevens, bijvoorbeeld omdat een bestand versleuteld is opgeslagen en de digitale sleutel is kwijtgeraakt of doordat een USB-stick wordt verloren;

[redacted]

B. Wat moet de medewerker doen in het geval van een incident of datalek?

Alle medewerkers moeten een incident of datalek kunnen herkennen én moeten weten hoe vervolgens te handelen. Wordt een incident of datalek vermoed of vastgesteld, dan dient er onmiddellijk contact te worden opgenomen met [naam coördinator of leidinggevende]. [Hij/Zij] onderzoekt of er sprake is van een datalek. In deze beoordeling wordt de volgende informatie meegenomen:

[redacted]