Datalekprotocol [naam organisatie]

Versie [jaartal of nummer]

Een beveiligingsincident met persoonsgegevens ofwel 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]

- een enveloppe met daarin een of meer documenten met persoonsgegevens komt geopend retour;
- een e-mail met daarin persoonsgegevens wordt aan de verkeerde ontvanger gestuurd;
- een bijlage met daarop persoonsgegevens bij een mail betreft niet de geadresseerde van die mail.

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.

[redacted]

- een enveloppe komt ongeopend retour afzender;
- een versleutelde e-mail met daarin persoonsgegevens is aan de verkeerde ontvanger gestuurd, maar het staat vast dat de sleutel niet is ontvangen door deze ontvanger.

Een beveiligingsincident of datalek kan ontstaan bij/door:

- moedwillig handelen of nalaten, bijvoorbeeld een hack;
- verlies van persoonsgegevens, bijvoorbeeld omdat een bestand versleuteld is opgeslagen en de digitale sleutel is kwijtgeraakt of doordat een onbeveiligde USB-stick of tablet is gestolen;

[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. Daarover bent u of zult u worden geschoold.

[redacted]