# Procedure datalekken.

Als medewerker of deelnemer heeft u uw persoonsgegevens aan CITAVERDE College toevertrouwd. Iedereen moet erop kunnen vertrouwen dat zijn persoonsgegevens (data) voldoende worden beveiligd. Slechte beveiliging kan leiden tot een datalek en vervolgens tot misbruik van deze gegevens. Bijvoorbeeld voor identiteitsfraude.

Om datalekken te voorkomen, moeten bedrijven en overheden die persoonsgegevens gebruiken deze beveiligen door passende technische en organisatorische maatregelen te nemen.

Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Onder een datalek valt dus niet alleen het vrijkomen (lekken) van gegevens, maar ook onrechtmatige verwerking van gegevens.. Voorbeelden van datalekken zijn: een kwijtgeraakte USB-stick met persoonsgegevens, een gestolen laptop of een inbraak in een databestand door een hacker.

Dit houdt in dat we als CITAVERDE College moderne techniek moeten gebruiken om persoonsgegevens te beveiligen en dat we niet alleen naar de techniek kijken, maar ook naar hoe we als organisatie met persoonsgegevens omgaan. Wie heeft er bijvoorbeeld toegang tot welke gegevens?

**Meldplicht datalekken**

Wanneer door welke reden dan ook data in verkeerde handen komen dan hebben organisaties de plicht om van een datalek direct melding te maken bij de Autoriteit Persoonsgegevens. De procedure die CITAVERDE College volgt in geval van een datalek is via de volgende link beschikbaar
http://bit.ly/citaverdeproceduredatalekken