

Netwerk DAK bewaart de volgende persoonsgegevens:

-Naam, email adres en telefoonnummer van beroepskrachten/coördinatoren van aangesloten organisaties met het doel om hen uit te nodigen voor bijeenkomsten en hen te informeren over relevante nieuwtjes en ontwikkelingen.

-Naam en email adres van penningmeesters dan wel degenen die zorgen voor de betaling van de contributie met het doel om de factuur van de contributie toe te zenden.

-Naam en email adres van deelnemers aan regionale en landelijke bijeenkomsten met het doel om de aanmelding te bevestigen en hen voor een volgende bijeenkomst uit te nodigen.

-Naam, emailadres en telefoonnummer van relevante contactpersonen met het doel om met hen te overleggen of hen te benaderen voor vragen of ideeën

-Email adressen van personen die zich geabonneerd hebben op de nieuwsbrief met het doel hen de nieuwsbrief toe te zenden. Enkel het email adres is geregistreerd. Toegang is alleen mogelijk voor degenen die kunnen inloggen op het cms van www.netwerkdak.nl.

Weten wat Netwerk DAK bewaart

In de email handtekening van de secretariaatsmedewerkers komt de volgende regel:

Persoonlijke gegevens worden vertrouwelijk behandeld. Lees het privacybeleid op www.netwerkdak.nl

Wie heeft toegang tot persoonsgegevens?

De betaalde medewerkers hebben toegang tot de persoonsgegevens. De gegevens zijn opgeslagen op de drie laptops en back up-media die voor de medewerkers door Netwerk DAK zijn aangeschaft en die alleen voor deze medewerkers toegankelijk zijn. De informatie staat goed beveiligd in de cloud via het programma Office 365 Premium. Gegevens van coördinatoren van de aangesloten organisaties worden eenmalig aan een drukker verstrekt ten behoeve van het verzenden van de uitnodiging van de jaarlijkse landelijke netwerkdag.

Een Functionaris gegevensbescherming is niet noodzakelijk.

Een PIA is niet noodzakelijk

Handeling bij datalek

De coördinator is verantwoordelijk voor het volgen van de procedure in geval van een datalek.

In kaart wordt gebracht:

- de aard van de inbreuk;
- de instanties of persoon waar meer informatie over de inbreuk kan worden verkregen;
- de aanbevolen maatregelen om de negatieve gevolgen van de inbreuk te beperken;
- een beschrijving van de geconstateerde en de vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens;
- de maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen;
- wie de melding doet bij de Autoriteit Persoonsgegevens binnen 24 uur na ontdekking.