AVG en Netwerk DAK

Aangepast maart 2020

Dossier: Hoe maak je jouw organisatie AVG-bestendig? Een 7-stappenplan Bron NOV-website

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing voor alle organisaties die gegevens van personen (persoonsgegevens) in een bestand bewaren. Deze organisaties moeten zich aan de regels in deze nieuwe verordening houden. Dat geldt zowel voor het bewaren in digitale bestanden als in mappen op een plank. Ook deze laatste moeten voortaan veilig worden opgeborgen zonder dat vreemden daar bij kunnen. Met onderstaande zeven stappen maak je jouw organisatie AVG-bestendig!

Stap 1: Ga waarom, hoe en wat na

Ga na welke persoonsgegeven worden verzameld en waar die worden bewaard. In de nieuwe AVG zijn ook vrijwilligersorganisaties verplicht te inventariseren wat ze vastleggen én te registreren welke persoonsgegevens ze hoe vastleggen. Ook moeten ze bedenken of dat wat ze opslaan wel functioneel is; waarom leggen ze welke gegevens vast. Dit houdt in dat je alleen persoonsgegevens vastlegt die je nodig hebt en dat je ze alleen gebruikt waarvoor je ze verzamelt.

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 regionale bijeenkomsten en hen te informeren over relevante nieuwtjes en ontwikkelingen.

Naam en email adres van penningmeesters danwel degenen die zorgt voor de betaling van de contributie met het doel om de factuur van de contributie toe te zenden.

Deelnemers aan regionale en landelijke bijeenkomsten met het doel om de aanmelding te bevestigen en hen voor een volgende bijeenkomst uit te nodigen.

Relevante contactpersonen in het veld met het doel om 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 in het account van Netwerk DAK bij La Posta.

De website van Netwerk DAK is gekoppeld aan Google analytics.

Denk bijvoorbeeld aan de voetbalvereniging die standaardadressen (straatnaam, postcode, huisnummer) van de leden in een bestand bewaard terwijl alle communicatie per telefoon, sociale media en digitale nieuwsbrief gaat. Deze clubs hoeven helemaal geen straat en huisnummer te bewaren. Het zal even wennen zijn maar hoe minder informatie er over personen bewaard wordt, hoe moeilijker gegevens herleidbaar zijn naar een persoon en hoe minder kans op schending van de privacy.

Stap 2: Laat weten wat je bewaart

Netwerk DAK

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

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

Onveranderd maar wel van belang is dat betrokkenen toestemming geven voor het gebruik van hun persoonsgegevens. Alleen wanneer daar een dringende reden van algemeen belang of wetgeving voor is, kunnen persoonsgegevens zonder toestemming worden opgeslagen. Nieuw is dat de betrokkenen moet weten dat zijn persoonsgegevens worden verwerkt en met welk doel. Zij hebben het recht hun gegevens in te zien en aan te (laten) passen . Bij verenigingen is helder dat persoonsgegevens noodzakelijk zijn voor het lidmaatschap en om deel te nemen aan de activiteiten. Dit laatste geldt ook voor deelname aan activiteiten van een stichting.

Pas op met bijzondere persoonsgegevens
Dit zijn persoonsgegevens van gevoelige aard zoals godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging of politieke partij, …

Stap 3: Vastleggen hoe de organisatie met de data omgaat

Organisaties hebben een verantwoordingsplicht in de nieuwe AVG. Dat betekent dat organisaties vastleggen wie verantwoordelijk is voor de data, aan wie informatie wordt verstrekten ook op welke computer deze wordt opgeslagen en op welke wijze deze wordt beschermt tegen virussen en hacken.

Netwerk DAK
De betaalde medewerkers hebben toegang tot de persoonsgegevens. De gegevens zijn opgeslagen op de vier laptops 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 algemeen drukwerk zoals uitnodigingen en kerstkaarten.

Niet onbelangrijk; zorg dat de data maar op één computer of één systeem staan. Verspreiding van data over verschillende computers of systemen zonder dat dat is vastgelegd kan uitgelegd worden als datalekken. Er moeten procedures worden opgesteld om personen toegang te geven tot de informatie. Met externe gebruikers van de bestanden, zoals drukkers, verspreiders van de nieuwsbrieven en bijvoorbeeld de koepelorganisatie, moeten overeenkomsten worden opgesteld voor het gebruik van gegevens; de zogenoemde verwerkersovereenkomst (zie verwerkersovereenkomst). In deze overeenkomsten moeten bijvoorbeeld ook afspraken gemaakt worden over het vernietigen van de gegevens na gebruik. Ook wanneer het om de koepelorganisatie gaat, moeten afspraken gemaakt worden over het gebruik van de bestanden. De organisaties maken immers afspraken met de leden over het zorgvuldig bewaren van hun gegevens en daar kan een organisatie op aangesproken worden. (zie privacybeleid)

Stap 4: Stel zo nodig een functionaris voor de gegevensbescherming (FG) aan

Een Functionaris gegevensbescherming is niet noodzakelijk.

Dit is niet verplicht voor alle organisaties. Wel voor overheids- en publieke organisaties, organisaties die persoonsgegevens analyseren (profiling) en wanneer bijzondere persoonsgegevens worden opgeslagen. Voor organisaties waarvoor een FG niet verplicht is, kan het wel handig zijn een FG aan te stellen. De FG is de centrale persoon die alle persoonsgegevens van de club beheert. Deze FG heeft zeggenschap over de bestanden en legt verantwoording af aan de verantwoordelijke beheerder, meestal het bestuur. Deze persoon beslist in opdracht van het bestuur over hoe bestanden worden opgeslagen en de procedure voor het beschikbaar stellen van de gegevens. Ook bestuursleden kunnen alleen via van tevoren vastgelegde procedures gegevens gebruiken. De FG zorgt er ook voor dat de virusscan op orde is en dat de computer beschermd is tegen hacken.

Stap 5: Privacy Impact Assessment (PIA)

Een PIA is niet noodzakelijk

Hiermee breng je in beeld wat de gevolgen zijn van het verzamelen van persoonsgegevens voor de personen zelf. Dit is afhankelijk van wat met de gegevens gedaan wordt. Wanneer de gegevens verzameld worden voor het versturen van de contributiebrief of een nieuwsbrief is het effect dat mensen lid blijven van de organisatie of dat ze geïnformeerd zijn over de organisatie. Niet voor alle bestanden met persoonsgegevens hoeft daarom een PIA gedaan te worden. Alleen wanneer:

Met de persoonsgegevens systematisch persoonlijke aspecten worden geëvalueerd (profiling)

Op grote schaal bijzondere gegevens worden verwerkt (zie stap 1)

Personen gevolgd worden in publieke ruimte (b.v. door camera toezicht)

Voor de meeste vrijwilligersorganisaties is een formele PIA niet nodig. Vooral niet omdat alleen contactgegevens verzameld worden en geen persoonskenmerken.

Stap 6: Vrijwilligers informeren of opleiden

Vrijwilligers hebben geen toegang tot de informatie

Het is niet de bedoeling dat wanneer je de gegevensbescherming zorgvuldig in beleid en procedures hebt geregeld, de eerste de beste vrijwilliger met persoonsgegevens die nodig zijn bij de uitoefening van de zijn/haar functie, te koop gaat lopen. Ook dat zijn datalekken. Dit kan gaan om gegevens uit de bestanden van de organisatie zelf, maar ook om informatie die een vrijwilliger van een deelnemer of ouder heeft gekregen.

Stap 7: Procedure opstellen voor het melden van datalekken

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

Elke organisatie die persoonsgegevens opslaat, is verplicht datalekken te melden binnen 72 uur na ontdekking. Om dit zorgvuldig te doen is het handig vooraf procedures af te spreken. Hierin staat:

We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben.

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.

Meldingen kunnen digitaal gedaan worden bij het meldloket van de Autoriteit Persoonsgegevens: http://datalekken.autoriteitpersoonsgegevens.nl

Wie controleert?

In Nederland controleert de Autoriteit Persoonsgegevens of organisaties voldoen aan de Algemene Verordening Gegevensbescherming. De Autoriteit Persoonsgegevens kan ook boetes opleggen wanneer na waarschuwingen een organisatie het beleid rond bescherming persoonsgegevens niet verbetert.