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

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 op geborgen 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.

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

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. Zijn 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

Verwerken van bijzondere persoonsgegevens is verboden, tenzij hiervoor een wettelijke uitzondering is of de persoon daar uitdrukkelijk tostemming voor heeft gegeven. Dit zijn persoonsgegevens van gevoelige aard zoals godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging of politieke partij, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, genetische en biometrische kenmerken. Onder deze laatste vallen vingerafdrukken, stem, handschrift, geometrie van de handomtrek en scans van netvlies, iris en gelaat.

Ook medische informatie, bijvoorbeeld over diabetes of allergieën, mag je alleen opslaan als er een wettelijke uitzondering is. Organisaties hebben nu de neiging deze informatie automatisch op te slaan in een bestand. Dat is niet langer toegestaan. Deze informatie moet dus iedere keer gevraagd voor activiteiten waarbij dat van belang is.

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.

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

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.

Voor organisaties die verplicht een Functionaris Gegevensbescherming (FG) moeten aanstellen heeft deze formeel de volgende verplichting:

- FG's mogen alleen handelen in opdracht van de verantwoordelijke;
- FG's worden verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die zij verwerken in opdracht van en verantwoordelijke;
- FG's moeten passende technische en organisatorische beveiligingsmaatregelen nemen die een passend beschermingsniveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen. FG's moeten uitgebreide kennis hebben omtrent hun informatiesystemen en de typen data die zij verwerken (is er sprake van bijzondere persoonsgegevens?);
- FG's mogen geen sub-FG's inschakelen zonder toestemming van de verantwoordelijke, wanneer sub-FG's worden ingezet moet de FG de nodige technische en organisatorische maatregelen nemen om de veiligheid en integriteit van de data te garanderen;
- FG's moeten de verantwoordelijke onmiddellijk op de hoogte stellen van een datalek. De termijn voor 'onverwijld' in de Nederlandse wetgeving wordt in de Wet Meldplicht datalekken vastgesteld op 72 uur na ontdekking van het incident;
- FG's zijn verplicht medewerking te verlenen aan verzoeken van de Autoriteit Persoongegevens;
- In bepaalde gevallen moet de FG een Privacy Impact Assessment uitvoeren. Dat is in ieder geval zo bij profiling, het verwerken van bijzondere persoonskenmerken en opslaan van camerabeelden met personen erop.

Stap 5: Privacy Impact Assessment (PIA)

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

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

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:

- Wat een datalek is;
  We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, een gestolen geprinte ledenlijst of cliëntgegevens. Andere voorbeelden zijn cyberaanvallen, verkeerd verzonden e-mail, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.
- Bij wie in de organisatie een datalek gemeld moet worden;
- Wie binnen de organisatie nog meer geïnformeerd moet worden;
- Wie checkt wat er gelekt is;
- Hoe in kaart gebracht wordt wat de gevolgen zijn voor de personen van wie de persoonsgegevens gelekt zijn;
- Welke gegevens nodig zijn voor de melding. De melding moet in ieder geval bestaan uit:
  - 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.