De AVG voor beginners

Wat is de AVG?
De AVG staat voor de nieuwe Europese privacywet Algemene Verordening Gegevensbescherming ofwel GDPR (General Data Protection Regulation), die in de hele EU geldig is. De AVG gaat 25 mei 2018 in werking. Alle verenigingen moeten dan aan de eisen van de AVG voldoen.
De AVG vervangt de huidige Wet Bescherming Persoonsgegevens, die in 2001 inging. Het Vrijstellingsbesluit bepaalde dat verenigingen onder voorwaarden niet aan artikel 27 van de WBP hoefden te voldoen. Je komt dit nog veel op internet tegen, maar het besluit is niet meer geldig sinds 31-12-2017.

Uitgangspunten van de AVG zijn dat persoonsgegevens met zorg behandeld dienen te worden en geheim dienen te blijven. Wie persoonsgegevens toch openbaar maakt zonder toestemming loopt kans een boete te krijgen.
Met de AVG wordt beoogd dat ongeoorloofde verspreiding van persoonsgegevens wordt voorkomen.
Om de privacy goed te borgen zijn vergaande maatregelen nodig.

Hoe bereid je je voor op 25 mei 2018?
Zodra je iemands naam op een lijstje zet, die je vaker dan een enkele keer gebruikt, verwerk je persoonsgegevens. De AVG eist dat je in een *privacyreglement* exact omschrijft welke gegevens je bewaart en wat je ermee doet. Dat reglement moet openbaar op je website staan. Als je geen website hebt moet je dit reglement aan nieuwe leden geven voordat zij zich opgeven als lid. Ook cookies horen bij privacy. Zodra je een foto plaatst op je website of een filmpje via Youtube deelt op je website worden er cookies geplaatst. Dat moet je noemen. Als je een mogelijkheid hebt voor leden om in te loggen worden er functionele cookies geplaatst. In het reglement moet je aangeven wat die cookies doen. De beschrijving in het privacyreglement moet compleet zijn, want je mag niets anders met de persoonsgegevens doen dan wat in het privacyreglement staat.

Je moet ook een *privacybeleid* hebben. Daarin beschrijf je precies wat de gang van zaken is binnen je afdeling of fotoclub. Wie mag de gegevens inzien en bewerken? Hoe worden gegevens vernietigd als ze niet meer nodig zijn? Hoe is je computer beveiligd zodat is gewaarborgd dat niemand anders toegang tot de gegevens kan krijgen? Dit dient bij alle personen die met persoonsgegevens te maken hebben goed tussen de oren te zitten. Zij moeten op de hoogte zijn van de regels en zich er aan houden.

Een *register* bijhouden is nodig als de verwerking niet incidenteel is (verantwoordingsplicht). Een ledenadministratie is niet incidenteel. Het register moet direct worden getoond als de Autoriteit Persoonsgegevens daarom vraagt. Dit register is de grootste klus. Iedere verwerking, bestand en formulier moet worden beschreven en gedocumenteerd.

Een functionaris gegevensbescherming aanstellen is niet nodig. Dat is alleen verplicht voor overheden en organisaties, die aan profilering doen of als bijzondere persoonsgegevens, zoals ras of geloofsovertuiging, worden geregistreerd.

Wat mag je met persoonsgegevens doen binnen je vereniging?
Het antwoord is kort: Niets, tenzij er een wettelijke grondslag is. De enige wettelijke grondslag die voor fotoclubs van toepassing is, is Toestemming. Degene over wie het gaat heet in de AVG de Betrokkene. Hij dient die toestemming vooraf, vrijelijk, specifiek, geïnformeerd en ondubbelzinnig te geven, bijvoorbeeld door een schriftelijke verklaring. Dat kan een e-mail zijn. Een mondelinge verklaring mag ook, maar als er problemen zijn is dat moeilijk te bewijzen.

Advies: Zet op het aanmeldingsformulier een verklaring en laat de Betrokkene die tekenen.

Je mag alleen die persoonsgegevens verzamelen die noodzakelijk zijn voor het uitvoeren van een taak. Een ip-adres mag je bij een bezoek aan de website niet opslaan als dat niet noodzakelijk is. Iemands geboortedatum mag je ook niet vragen als je die niet hoeft te weten. Als het nodig is om een kaartje te sturen als de Betrokkene jarig is mag het wel als dit in het privacyreglement is beschreven.

De Fotobond heeft een naam, adres en mailadres nodig. Het e-mailadres is verplicht, maar wie geen e-mailadres heeft kan toch lid worden. Hij kan dan alleen geen informatie van de Fotobond ontvangen, zoals een nieuwsbrief. Voor een club is een adres handig als je een lid dat ziek is een kaartje wilt sturen of een bloemetje.

Het moet tot je beleid behoren dat je alleen die persoonsgegevens vraagt die noodzakelijk zijn.
Je mag alleen persoonsgegevens verwerken als de verwerking rechtmatig, behoorlijk en transparant is. Er moet dus transparantie (hij moet weten wat er met de persoonsgegevens gebeurt en welke gegevens dat zijn) naar de Betrokkene zijn en er moet toestemming van de Betrokkene zijn. Er worden wettelijke eisen gesteld aan transparantie. Er moet in eenvoudige en duidelijke taal worden uitgelegd wanneer persoonsgegevens worden verzameld en wat de rechten van Betrokkene zijn, namelijk recht op inzage, recht op rectificatie, recht om te worden vergeten, recht op beperking van de verwerking, kennisgevingsplicht, recht op overdraagbaarheid van gegevens.

Een verwerking is rechtmatig als er toestemming van de betrokkene is of de verwerking is noodzakelijk op verzoek van overeenkomst.

Persoonsgegevens mogen volgens de AVG alleen voor de volgende doeleinden worden verwerkt:

- activiteiten die, gelet op de doelstelling van de vereniging gebruikelijk zijn;
- andere dan de hierboven bedoelde gebruikelijke activiteiten, als die door de ledenvergadering zijn goedgekeurd;
- het verzenden van informatie aan de leden of begunstigers;
- het bekend maken van informatie over leden of begunstigers en activiteiten van de vereniging na instemming van de ledenvergadering, voor zover aanwezig, op de eigen website;
- foto’s en videobeelden met of zonder geluid van activiteiten van de vereniging;
- het berekenen, vastleggen en innen van contributies en giften (inclusief het in handen van derden stellen van vorderingen);
- andere activiteiten van intern beheer;
- het behandelen van geschillen;
- het doen uitoefenen van accountantscontrole.

Je mag alleen de volgende gegevens registreren (als daar een goed omschreven doel voor is vastgesteld):

- naam, voornamen, voorletters, titulatuur, geslacht, geboortedatum, adres, postcode, woonplaats, telefoonnummer en soortgelijke voor communicatie benodigde gegevens (bijvoorbeeld het e-mailadres), evenals het bankrekeningnummer van het lid of de begunstiger;
- een lidnummer, indien dat geen andere informatie bevat dan de bij het vorige punt bedoelde gegevens;
- de bij het eerste punt bedoelde gegevens van de ouders, voogden of verzorgers van minderjarige leden of begunstigers;

- gegevens die betrekking hebben op het lidmaatschap of de begunstiging. Hieronder zijn begrepen gegevens over de aard van het lidmaatschap of de begunstiging (bijvoorbeeld de datum van aanvang van het lidmaatschap en het soort lidmaatschap), de functie binnen de vereniging, stichting of publiekrechtelijke beroepsorganisatie (bijvoorbeeld de functie binnen het bestuur) en de deelname aan de activiteiten van de vereniging (bijvoorbeeld de beschikbaarheid voor activiteiten of deelname aan een festival of cursus);
- gegevens voor het berekenen, vastleggen en innen van contributies en giften.

De gegevens mogen alleen worden verstrekt aan:

- de leden of begunstigers;
- de ouders, voogden of verzorgers van minderjarige leden of begunstigers;
- degenen, inclusief derden, die belast zijn met de hierboven beschreven doeleinden, of leiding geven aan de hierboven beschreven doeleinden, of noodzakelijk zijn betrokken bij de hierboven beschreven doeleinden;
- anderen, indien: het lid of de begunstiger zijn ondubbelzinnige toestemming heeft verleend voor de gegevensverwerking, of de gegevensverwerking noodzakelijk is voor de nakoming van een wettelijke plicht door de vereniging, of de gegevensverwerking noodzakelijk is vanwege een vitaal belang van het lid of de begunstiger (bijvoorbeeld een dringende medische noodzaak), of de gegevens verder worden verwerkt voor historische, statistische of wetenschappelijke doeleinden. Voorwaarde hierbij is dat de vereniging ervoor zorgt dat de gegevens ook alleen voor deze specifieke doeleinden verder worden verwerkt.

Je mag de leden van je club dus een ledenlijst geven.

Voor websites gelden aanvullende regels:

- Gegevens op de website van de vereniging worden slechts verstrekt aan: de leden of begunstigers; de ouders, voogden of verzorgers van minderjarige leden of begunstigers; degenen, waaronder begrepen derden, die belast zijn met of leiding geven aan de hierboven bedoelde activiteiten of die daarbij noodzakelijkerwijs zijn betrokken, voor zover zij daartoe door het bestuur zijn geautoriseerd. Dit betekent dat alleen na inloggen deze gegevens voor leden beschikbaar mogen zijn.
- Het bestuur draagt zorg voor een adequate toegangsbeveiliging van de website, alsmede voor een afdoende bescherming van persoonsgegevens voor verdere verwerking door zoekmachines.
- De gegevens op de website worden onverwijld verwijderd wanneer de betrokkene of diens wettelijke vertegenwoordiger daarom verzoekt.

Een ledenlijst openbaar op de website zetten mag dus niet. De naam van de winnaar van het clubfilmfestival openbaar maken mag ook niet. Een foto van de winnaar op de website plaatsen mag ook niet. Dit mag wel als er een wettelijke grondslag is zoals toestemming. De betrokkene behoudt altijd het recht om de persoonsgegevens te laten verwijderen.

Wat is een datalek?
We spreken van een inbreuk in verband met persoonsgegevens of datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. (datalekken.html). Ook het onrechtmatig verwerken van gegevens valt hieronder.
Een datalek kan ontstaan door uitgelekte computerbestanden, maar een gestolen geprinte lijst met persoonsgegevens kan dat ook zijn. Andere voorbeelden zijn: e-mail verzonden naar verkeerde adressen, gestolen of verloren laptops, afgedankte niet-schoongemaakte computers en verloren usb-

sticks. Een zoekgeraakte privételefoon valt niet onder een datalek. Een afgesloten website met persoonsgegevens die per ongeluk openstaat is wel een datalek.

Voorkom datalekken door afdoende beveiliging van gegevens, het zorgvuldig bewaren van gegevens, zoals papieren lijsten, het zo min mogelijk verzamelen van persoonsgegevens en het verwijderen van gegevens, als ze niet meer nodig zijn.

Er is op internet veel informatie over het melden van datalekken bij de Autoriteit Persoonsgegevens. Dit geldt niet als het onwaarschijnlijk is dat de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen (artikel 33 AVG). Bij fotoclubs zal dat vrijwel altijd het geval zijn.

Uitwisselen van persoonsgegevens
Zolang persoonsgegevens binnen een club blijven is het allemaal redelijk overzichtelijk.
Door de structuur van de Fotobond worden gegevens uitgewisseld tussen Fotobond, afdelingen en clubs. De clubs leveren gegevens aan de afdelingen en de Fotobond en de Fotobond verstrekt gegevens aan afdelingen, clubs en persoonlijke leden.

Een hostingprovider wordt ook als Verwerker aangemerkt. Als je een website hebt moet je met de provider een Verwerkersovereenkomst sluiten.

Daarom moeten er Verwerkersovereenkomsten worden opgesteld tussen de verenigingen. Daarin wordt verklaard dat persoonsgegevens geheim blijven en alleen voor het doel worden gebruikt, die in de overeenkomst staan. De Fotobond zal Verwerkersovereenkomsten met de aangesloten afdelingen en clubs sluiten. En uiteraard met externe verwerkers van gegevens, zoals voor de verzending van Fotobond in Beeld.

Gegevens moeten binnen de EU blijven, tenzij…
Dat lijkt niet zo ingewikkeld, maar dat is het wel.
Alle landen van de EU hebben dezelfde privacyregels. Daar zijn Noorwegen, Liechtenstein en IJsland aan toegevoegd, omdat zij de AVG in hun wetgeving verankeren. Daarbuiten mogen persoonsgegevens alleen worden doorgegeven als er een passend beschermingsniveau is.
Er is een landenlijst, waar op staat welke landen een passend beschermingsniveau bieden. Voor de VS geldt dit alleen als dit gebeurt op grond van de EU-VS privacy shield. Dat is een akkoord, waarbij de bedrijven op deze lijst verklaren dat zij geen persoonsgegevens van Europese burgers delen met de Amerikaanse geheime dienst.

Google en Microsoft staan op deze lijst van de EU-VS privacy shield, maar Apple niet. (www.privacyshield.gov). Dit betekent dat je persoonsgegevens mag opslaan op Google Drive en One Drive, maar niet in iCloud van Apple.
Gmail en Outlook mag je gebruiken om persoonsgegevens te versturen.

Informatie beschikbaar gesteld door NOVA Federatie (Nederlandse Organisatie van Audiovisuele Amateurs). De Fotobond werkt samen met de NOVA en de NVBG (Nederlandse Vereniging voor Beeld en Geluid) aan modellen die gebruikt kunnen worden binnen de drie verenigingen.