

Algemene info over AVG voor Probusclubs (versie 19 april 2018)

AVG

(Uitvoeringswet Algemene Verordening Gegevensbescherming)

Wat is de AVG?

De AVG is de Nederlandse uitwerking van de nieuwe Europese privacywet GDPR (General Data Protection Regulation), die in de hele EU geldig is. De Uitvoeringswet AVG voorziet in de nationale regels die nodig zijn ter uitvoering van de GDPR. De AVG vervangt bovendien de huidige Wet Bescherming Persoonsgegevens (WBP) van 2001 ingang. De AVG treedt **25 mei 2018** in werking

Alle verwerkers van persoonsgegevens, moeten voldoen aan de eisen van de AVG, dus ook alle verenigingen, groot en klein.

De AVG kent geen vrijstellingsbesluit zoals dat van de WBP. Het Vrijstellingsbesluit van WBP 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. Verenigingen waren vrijgesteld van de plicht om de verwerking van persoonsgegevens aan te melden bij de Autoriteit Persoonsgegevens. Het vrijstellingsbesluit is vervallen en dus moeten verenigingen ook een **Verwerkingsregister** bijhouden.

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.

Wat zijn persoonsgegevens?

Zodra je iemands naam op een lijstje zet, die je vaker dan een enkele keer gebruikt, verwerk je persoonsgegevens. Als je persoonsgegevens verwerkt moet je een **privacy beleid** hebben. Daarin beschrijf je precies wat de gang van zaken is binnen je vereniging. 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? Alle personen binnen de vereniging, die met persoonsgegevens te maken hebben, moeten op de hoogte zijn van en zich houden aan de regels.

De AVG eist voorts dat je in een **Privacy Reglement** exact omschrijft welke gegevens je bewaart en wat je ermee doet. Als je geen website hebt moet je dit reglement aan je (nieuwe) leden geven voordat zij zich opgeven als lid. Als je wel een website hebt moet je het publiceren op de website.

Een **Verwerkingsregister** 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 er bijzondere persoonsgegevens, zoals ras of geloofsovertuiging, worden geregistreerd.

Wat mag je met de persoonsgegevens doen?

Het antwoord is kort: in principe niets, tenzij er een wettelijke grondslag is. De belangrijkste wettelijke grondslag, die voor Probusclubs van toepassing is, is toestemming van de betrokkene. De betrokkene – dat is bij voorbeeld het lid van een Probusclub dat op de ledenlijst staat - 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 deze door betrokkene tekenen, of stel een verklaring op die het betrokken lid bij zijn installatie tekent.

Een vereniging mag een ledenlijst beschikbaar stellen aan de leden. Het is verstandig om de ledenvergadering eenmalig te verzoeken om daarmee in algemene zin in te stemmen, mocht dit nog niet gebeurd zijn.

Je mag alleen die persoonsgegevens verzamelen, die noodzakelijk zijn voor het uitvoeren van een taak. Zo mag je een IP- adres 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 voor de commissie Lief en Leed om een kaartje te sturen als de betrokkene jarig is mag het wel, als dit in het Privacy Reglement is beschreven.

Je mag dus alleen persoonsgegevens verwerken als de verwerking rechtmatig en transparant is. Er moet transparantie zijn (de betrokkene moet weten wat er met zijn/haar persoonsgegevens gebeurt en welke gegevens dat 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 welke 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 als de verwerking is noodzakelijk voor een wettelijke taak.

Persoonsgegevens openbaar maken mag niet. Daar valt een ledenlijst onder, maar ook het bekend maken van de naam van de winnaar van een wedstrijd en een foto van de winnaar op de website plaatsen. Dit mag wel als er een wettelijke grondslag is zoals toestemming van de betrokkene. De betrokkene behoudt altijd het recht om de persoonsgegevens te laten verwijderen. Het verspreiden van deze gegevens onder eigen leden mag wel als daar in de reglementen toestemming voor is gegeven door de ALV. Zet deze gegevens, verslagen en nieuwsbrieven dus achter een inlogcode.

Wat is een data lek?

We spreken van een inbreuk in verband met persoonsgegevens of van een data lek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Ook het onrechtmatig verwerken van gegevens valt hieronder.

Een data lek 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 data lek. Een besloten website met persoonsgegevens die per ongeluk openstaat is wel een data lek.

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. Als iemand een klacht indient bij de Autoriteit Persoonsgegevens over een data lek moet de Autoriteit Persoonsgegevens dit onderzoeken en dan moet de betreffende organisatie aantonen dat zij de nodige maatregelen heeft genomen om datalekken te voorkomen.

Uitwisselen van persoonsgegevens

Zolang persoonsgegevens binnen een club blijven is het allemaal redelijk overzichtelijk.

Als verwerkers worden ingeschakeld moeten verwerkersovereenkomsten worden opgesteld. Daarin wordt verklaard dat persoonsgegevens geheim blijven en alleen voor het doel worden gebruikt, dat in de overeenkomst staan. Stichting Probus Nederland zal een verwerkersovereenkomst sluiten met Mediaver-sa als provider van onze website; Probusclubs zelf hoeven dit niet te doen.

Gegevens blijven binnen de EU

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, waarop 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, maar Apple niet. Dit betekent dat je persoonsgegevens mag opslaan op Google Drive en One Drive, maar bijvoorbeeld niet in iCloud van Apple. Gmail en Outlook mag je gebruiken om persoonsgegevens te versturen.

Uitgebreidere informatie kunt u vinden op de website van de autoriteit persoonsgegevens <https://autoriteitpersoonsgegevens.nl/>.

Opgesteld door Probus Nederland,

Jan van Zoest, 19 april 2018