Nieuwe Privacyregels: Is uw club/vereniging AVG-bestendig?

Op 25 mei aanstaande treedt de Algemene Verordening Gegevensbescherming (AVG) in werking. Dit is een ingrijpende wet, die de nodige gevolgen heeft voor alle organisaties die persoonsgegevens verwerken. Iedere club, vereniging en stichting in Nederland heeft er dus mee te maken en daarom is het van belang dat u op 25 mei 2018 AVG-proof bent, want er is geen overgangsperiode en de boetes liegen er niet om! Ik heb daarom de nodige informatie verzameld en in onderstaande artikel een samenvatting geplaatst met daarin de belangrijkste informatie.

Een nieuwe wet

Deze nieuwe wet vervangt de Wet bescherming persoonsgegevens (Wpb) en zal binnen de gehele EU gelden. In grote lijnen is de nieuwe wet bedoeld dat personen geen nadeel ondervinden van dat gegevens over hen worden verzameld, verwerkt en gebruikt. De term persoonsgegevens is in deze erg ruim, het betreft namelijk niet alleen de gangbare gegevens, zoals naam, adres, woonplaats, e-mailadressen etc., maar ook aankoop gegevens (wat heeft .. gekocht) en bijvoorbeeld uw zoekgeschiedenis op internet (cookies).

Binnen de nieuwe wet wordt de positie van de betrokkenen (de mensen van wie gegevens worden verwerkt) versterkt en daarnaast krijgen organisaties (dus ook clubs, verenigingen en stichtingen) die persoonsgegevens verwerken meer verplichtingen. Een organisatie moet kunnen aantonen dat zij zich aan de wet houdt.

In dit artikel zal ik ingaan op de stappen die u als club, vereniging of stichting (ik spreek verder alleen over club als ik deze drie organisaties bedoel) dient te ondernemen om straks klaar te zijn voor de AVG. Daarnaast zal ik ook een aantal concrete voorbeelden behandelen.

Stappenplan

Als je in google AVG invoert komen er gelijk mega veel sites in beeld over dit onderwerp. Ook zijn er veel bedrijven die hier handig op inspringen. Er zijn ook bedrijven, die zich speciaal op verenigingen en stichtingen richten. Het is natuurlijk aan u zelf te beoordelen of u een (commerciële) partner in de arm neemt of dat u het zelf uitvoert. Mijn inschatting is dat de meeste clubs het goed zelf kunnen oppakken. Zoals ik al schreef, is de hoeveelheid sites die informatie verstrekken overweldigend, waardoor het risico bestaat dat je door de bomen het bos niet meer ziet. Daarom wijs ik op de site van de Autoriteit Persoonsgegevens (autoriteitpersoonsgegevens.nl). Hier kun je eigenlijk alle informatie terugvinden. De autoriteit persoonsgegevens heeft ook de 10 belangrijkste stappen op een rijtje gezet:

Stap 1: Bewustwording
Zorg dat alle relevante mensen (bestuurders en anderen die persoonsgegevens verwerken of gebruiken) in uw club op de hoogte zijn van de nieuwe privacyregels. Maak daarnaast een inschatting wat de impact van de AVG is op uw huidige processen en administratie.

Stap 2: Rechten van betrokkenen
De mensen van wie u persoonsgegevens verwerkt krijgen vanaf 25 mei 2018 meer en verbeterde privacyrechten. Zorg dat u daarop voorbereid bent zodat u op tijd en op de juiste manier kunt reageren.

Enkele belangrijke rechten zijn:
- Recht op inzage
- Recht op correctie en verwijdering
- Recht op dataportabiliteit (dit houdt in dat betrokkene zijn gegevens makkelijk moet kunnen krijgen en ze moeten makkelijk kunnen worden doorgegeven aan een andere organisatie indien de betrokkene dat wenst).

Stap 3: Overzicht verwerkingen
Breng uw gegevensverwerkingen in kaart. Leg vast welke persoonsgegevens u verwerkt en met welk doel u dit doel, waar deze gegevens vandaan komen en met wie u ze deelt. Vermeld in dit overzicht ook per categorie van gegevens op basis van welke wettelijke grondslag u deze gegevens verwerkt (gerechtvaardigd belang of toestemming van betrokkene).

Dit overzicht heeft een tweeledig doel. Allereerst kunt u het gebruiken voor de verantwoordingsplicht. U moet namelijk kunnen aantonen dat uw club in overeenstemming met de AVG handelt. Daarnaast kunt u het overzicht ook nodig hebben als betrokkenen hun privacyrechten uitoefenen.

Stap 4: Data Protection Impact Assessment
Onder de AVG kan het voorkomen dat u verplicht bent een Data Protection Impact Assessment (DPIA) uit te voeren. Dit is een overzicht waarmee u vooraf de privacyrisico's van een gegevensverwerking in kaart brengt. Voor zover ik kan inschatten is er binnen de NMF geen enkel lid dat hiervoor in aanmerking komt en dus laat ik deze stap verder voor wat 'ie is…

Stap 5: Privacy by design & privacy by default
Onder de AVG gelden een aantal verplichte uitgangspunten. Ga na hoe u deze beginselen binnen uw club kunt invoeren.

Pricacy by design houdt in dat u er al bij het ontwerpen van producten en diensten voor zorgt dat gegevens goed worden beschermt.

Privacy by default houdt in dat u technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat u, als standaard, alléén persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat u wilt bereiken.
Voorbeelden hiervan zijn:
- Laat een app, die u aanbiedt niet de locatie van gebruikers registreren als dat niet nodig is;
- Op uw website het vakje 'Ja, ik wil aanbiedingen ontvangen' niet vooraf aanvinken;
- Als iemand zich op uw nieuwsbrief wil abonneren niet meer gegevens vragen dan nodig is.

Stap 6: Functionaris voor de gegevensbescherming
Hoewel uw club hiertoe onder de AVG waarschijnlijk niet verplicht zal zijn, is het toch raadzaam om binnen uw club iemand hiervoor aan te stellen, hierdoor is het voor iedereen duidelijk tot wie men zich dient te wenden. Omdat het niet verplicht is, kunt u zelf bepalen welke taken en bevoegdheden de functionaris krijgt. Zorgt u er wel voor dat de functionaris voldoende bevoegdheden heeft om ervoor zorg te dragen dat uw club de AVG naar behoren naleeft.

Stap 7: Meldplicht datalekken
Elke organisatie die persoonsgegevens opslaat, is verplicht datalekken binnen 72 uur na ontdekking te melden. Om dit zorgvuldig te doen is het handig om hiervoor een procedure vast te leggen met daarin in ieder geval:

- Wat een datalek is (er is sprake van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Voorbeelden: uitgelekte computerbestanden, gestolen/verloren geprinte ledenlijst, cyberaanvallen, verkeerd verzonden e-mail, gestolen computer, afgedankte niet-schoongemaakte computers en verloren usb-sticks);
- Bij wie in de organisatie een datalek gemeld moet worden;
- Wie binnen de club 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 personen 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 de persoonsgegevens;
    - De maatregelen die de organisatie heeft genomen of voorstelt te nmen om deze gevolgen te verhelpen.
- Wie de melding doet bij de Autoriteit Persoonsgegevens.

De melding wordt digitaal gedaan bij het meldloket: http://datalekken.autoriteitpersoonsgegevens.nl

Stap 8: Bewerkersovereenkomsten
Vaak wordt er gebruik gemaakt van externe (IT-)dienstverleners (denk hierbij aan een online ledenadministratie, beheer van apps en hosting van websites). In bijna alle gevallen worden er via dergelijke diensten persoonsgegevens verwerkt. Zo'n dienstverlener wordt dan een 'bewerker' genoemd. U bent als verantwoordelijke verplicht om met deze partij een bewerkersovereenkomst te sluiten. Daarin leg je hoofdzakelijk afspraken vast die borgen dat de dienstverlener zorgvuldig met persoonsgegevens omgaat. Dat is erg belangrijk, want als club blijf je ook na inschakeling van een dienstverlener verantwoordelijk. Wordt er gebruik gemaakt van servers buiten de EU voor de dataopslag, dan is dit alleen toegestaan indien er bijzondere waarborgen zijn getroffen (EU-modelcontracten en/of Privacy Shield).

Stap 9: Leidende toezichthouder
Dit is alleen nodig indien uw club ook gevestigd is in andere EU landen. Zover mij bekend is dat bij de leden van de NMF niet het geval en daarom heb ik het enkel genoemd ter kennisname en ga ik hier niet verder op in.

Stap 10: Toestemming
De verwerking van sommige persoonsgegevens is verboden tenzij hiervoor een wettelijke uitzondering is of de persoon daar uitdrukkelijk toestemming voor heeft gegeven (denk hierbij aan gegevens van gevoelige aard zoals godsdienst, levensovertuiging, ras, politieke gezindheid, gezondheid, genetische en biometrische kenmerken [bijvoorbeeld: (pas)foto, vingerafdrukken, stemopname, scans van netvlies, iris en gelaat}). Mijn advies is om dergelijke gegevens niet te gebruiken en/of te verzamelen. U moet namelijk aan kunnen tonen dat u geldige toestemming heeft

gekregen van de betrokkene om deze gegevens te gebruiken. Voor de betrokkene moet het net zo makkelijk zijn om deze toestemming in te trekken als deze te geven.

Ledenadministratie

De ledenadministratie is bij de meeste clubs de centrale gegevensverzameling, waar persoonsgegevens worden verzameld en bewaard. De ledenadministratie omvat allerhande gegevens, zoals NAW gegevens, bankgegevens, contactgegevens etc. Daarom is het goed om hier verder op in te gaan.

In de ledenadministratie mag je uitsluitend persoonsgegevens opnemen voor zover daar een rechtmatig doel voor bestaat. Controleer dus of voor alle gegevens geldige grondslag aanwezig is (gerechtvaardigd belang, toestemming, contractuitvoering of wettelijke verplichting). Verzamel niet meer persoonsgegevens dan werkelijk nodig zijn voor het doel dat je nastreeft. Daarnaast mag je de gegevens niet zomaar voor een ander doel gebruiken dan waarvoor je ze hebt gekregen (voorbeeld: als je de geboortedatum vastlegt om te bepalen of iemand een jeugdlid is of niet, mag je deze niet gebruiken om hem te feliciteren met zijn verjaardag).

Indien je NAW-gegevens van de leden aan sponsors wilt verstrekken zodat zij commerciële boodschappen kunnen versturen, is een uitdrukkelijke toestemming van een lid vereist. Indien deze gegevensverstrekking in algemene zin door de ALV is goedgekeurd, heb je geen individuele toestemming meer nodig van de leden. Let op: Voor het verstrekken van e-mailadressen gelden strengere regels (SPAM-regels), hier is altijd een individuele toestemming van ieder lid noodzakelijk.

Een club mag in principe een ledenlijst beschikbaar stellen aan eigen leden. Ik raad wel aan om de ALV eenmalig te verzoeken om daarmee in algemene zin in te stemmen, mocht dit nog niet gebeurd zijn. De Autoriteit Persoonsgegevens stelt uitdrukkelijk dat het online publiceren van een ledenlijst slechts is toegestaan op een voor leden afgeschermde webpagina.

Persoonsgegevens van een uitgetreden lid mogen in principe niet langer dan twee jaar na einde van het lidmaatschap bewaard worden. Voor informatie die valt onder fiscale bewaarplicht geldt een langere bewaartermijn van zeven jaar.

Tenslotte is het van belang dat de ledenadministratie veilig bewaard wordt. Dit geldt niet alleen voor de digitale administratie, maar ook de papieren gegevens. Zorg dus voor goede technische en organisatorische beveiligingsmaatregelen, waarbij een afsluitbare kast voor de papieren administratie en wachtwoorden voor digitale bestanden wel het minimale is.

Vrijwilligers

Omdat de vereniging/club/stichting op vrijwilligers draait en normaliter geen werknemers heeft, is de gezagsverhouding ook anders en vindt er over het algemeen minder controle plaats. Onder de AVG is de club verantwoordelijk en dus verplicht te bewaken dat vrijwilligers persoonsgegevens verwerken zoals de club dit voorschrijft. Als de vrijwilliger tekort schiet, is de club aansprakelijk! Daarom enkele tips:

- Stel een beleid op en leg de werkprocessen vast en zorg dat deze goed gecommuniceerd worden met de vrijwilligers;
- Controleer (af en toe) of het beleid daadwerkelijk wordt nageleefd;
- Beperk de toegang tot de persoonsgegevens, zodat de vrijwilligers alleen toegang hebben tot gegevens die noodzakelijk zijn voor de uitvoering van hun taak;

- Zorg voor een tijdige beëindiging van de toegang tot informatie als vrijwilligers hun taken neerleggen. Zorg ook dat alle persoonsgegevens worden teruggegeven en waar nodig worden gewist van privéapparatuur van de vrijwilliger.

Nieuwsbrieven en andere elektronische mailings

Ik heb het hierboven al eens genoemd: de SPAM-regels. Deze gelden voor alle elektronische commerciële berichten (via e-mail en social media). Dit zijn bijzondere regels voor het versturen van "ongevraagde" berichten. Voor het versturen van dergelijke berichten heb je uitdrukkelijke en voorafgaande toestemming nodig van de ontvangen. (zgn. Opt-out, waarbij je niet vooraf om toestemming vraagt, maar wel de gelegenheid biedt om uit te schrijven, is onvoldoende). Teven moet je ontvangers altijd een eenvoudige gelegenheid bieden tot uitschrijving van deze berichten.

Omdat clubs hun leden moeten kunnen informeren over het reilen en zeilen binnen de vereniging, is hier een uitzondering gemaakt. Nieuwsbrieven, uitnodigingen voor ledenvergaderingen of de verenigingsevenementen enz. mogen zonder uitdrukkelijke toestemming van het lid worden verzonden, mits deze uitsluitend dergelijke berichten bevat en er geen commerciële elementen in zitten. Heb je advertenties van sponsoren in je nieuwsbrief of digitaal verenigingsblad staan, dan geldt deze uitzondering dus niet!

Publiceren van foto's en video's

Ook foto's en video's met een herkenbaar in beeld gebrachte betrokkene zijn persoonsgegevens! Voor het maken en publiceren heb je daarom toestemming nodig van de betrokkene. Voor zover ik heb kunnen nagaan kan volstaan worden met het op voorhand opnemen van een toestemmingsbepaling in de lidmaatschapsvoorwaarden of evenementvoorwaarden. Bij personen jonger dan 16 jaar heb je de toestemming van de ouder/wettelijk vertegenwoordiger nodig. Toch kan ook dan een in beeld gebrachte persoon zich verzetten tegen publicatie. In de regel zal je gehoor moeten geven aan dergelijke verzoeken, maar er zijn ook gevallen waarbij je gewoon de publicatie mag doorzetten. Wil je dit laatste dan raad ik je aan deskundig advies in te winnen.

Privacyverklaring

Een club, die met persoonsgegevens werkt, is wettelijk verplicht de betrokkenen te laten weten welke gegevens verwerkt worden en waarom. Hierbij dien je aan te geven welke persoonsgegevens je verwerkt, voor welk doel je dit doet en welke rechten betrokkene heeft ten aanzien van zijn persoonsgegevens. Vermeld deze privacy verklaring in ieder geval op je website, voeg deze toe aan een eventueel inschrijfformulier en verstrek hem samen met de statuten en huishoudelijk reglement aan ieder nieuw lid.

De club is verplicht om in haar privacyverklaring minimaal de volgende informatie te verstrekken:

- De officiële identiteits- en contactgegevens van de club;
- De soorten persoonsgegevens die worden verwerkt;
- Voor welke doeleinden die verwerkingen plaatsvinden en op welke grondslag dit plaatsvindt;
- Indien ze worden gedeeld met derden, vermeld dan welke derden dit betreft;
- Indien ze worden opgeslagen buiten de EU, vermeld dan welke maatregelen zijn getroffen om een passend beschermingsniveau te waarborgen;
- Welke rechten de betrokkene (onder bepaalde omstandigheden) heeft, namelijk het recht op inzage, correctie, verwijdering, dataportabiliteit en het recht van verzet tegen een bepaalde verwerking;
- Hoelang persoonsgegevens worden bewaard (of welke criteria daarvoor gelden);

- Indien voor bepaalde verwerkingen toestemming wordt gevraagd, de vermelding van deze te allen tijde mag worden ingetrokken door de betrokkene;
- Een vermelding dat iedere betrokkene het recht heeft om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- Als je de persoonsgegevens verwerkt ter uitvoering van een contract of een wettelijke verplichting, vermeldt dit dan en vermeldt dan tevens wat de consequentie is als een betrokkene dergelijke persoonsgegevens niet verstrekt (bijvoorbeeld: geen lid kunnen worden van de vereniging);
- Als je gebruik maakt van profilering of geautomatiseerde besluitvorming, vermeldt dit dan uitdrukkelijk.

<u>Cookies</u>

Als laatste wil ik ook nog even de cookies benoemen. Veel websites maken hier tegenwoordig gebruik van. De regels hieromtrent staan opgenomen in de Telecommunicatiewet en worden ook wel de 'cookiewet' genoemd. Het betreffen hier regels omtrent het uitlezen en plaatsen van informatie op randapparatuur zoals mobiele telefoon, tablet of computer.

Er zijn drie soorten cookies:

1. Technisch noodzakelijke cookies. Een goed voorbeeld hiervan is het winkelwagentje in de webshop;
2. Kwaliteits- en of effectiviteitscookies. Dit zijn cookies waarmee de kwaliteit en de effectiviteit van een website worden verbeterd. Ook affiliate-cookies vallen onder deze groep (de adverteerder kan dan bijhouden welke advertentie daadwerkelijk tot de aankoop van een product heeft geleid);
3. Tracking cookies: deze cookies volgen het internetgedrag van de gebruiker.

Je bent verplicht de gebruikers erop te wijzen dat je cookies gebruikt en daarnaast moet de gebruiker toestemming geven voordat de cookies worden geplaatst. De informatie aan de gebruiker moet minimaal de volgende gegevens bevatten:

- De naam van de partij die de cookies plaatst;
- Het doel waarvoor de cookies worden gebruikt (bijvoorbeeld: tracking, gerichte advertenties of verbetering van de website);
- Het type cookie dat door of via de website wordt geplaatst;
- Het gebruik van andere relevante technieken. (bijvoorbeeld Javascript en Web Beacons);
- De eventuele impact die de cookies kunnen hebben op de privacy van de gebruiker.

Er zijn drie gevallen waarin geen toestemming nodig is en ook geen informatie hoeft te worden verschaft:

- De cookies zijn technisch noodzakelijk om elektronische communicatie mogelijk te maken;
- De cookies zijn nodig om een door de gebruiker gevraagde dienst te leveren;
- De cookies zijn bedoeld om informatie te verkrijgen over de kwaliteit of effectiviteit van de website en hebben geen of geringe gevolgen voor de privacy van de gebruiker.

Januari 2018,
Peter-Martijn Hellemons
Voorzitter Nederlandse Modelspoor Federatie