Stappenplan AVG voor verenigingen

Algemeen

1. *Persoonsgegevens: inventarisatie en registratie*
   Ga na welke persoonsgegevens worden verzameld en waar die worden bewaard. Ga hierbij ook na waarvoor de gegevens worden verzameld. Denk bijvoorbeeld aan: ledenadministratie, personeelsadministratie, nieuwsbrief, etc. De AVG verplicht organisaties om te inventariseren en registreren wat er met persoonsgegevens gebeurt.

   In de registratie moet worden opgenomen wie verantwoordelijk is, waarom de gegevens verwerkt worden, welke grondslag voor verwerking (uitvoering van een overeenkomst, toestemming of een gerechtvaardigd belang) er is en hoe lang de gegevens bewaard worden.

   Ga bij de inventarisatie meteen na welke gegevens misschien niet hoeven/mogen worden opgeslagen. Gegevens mogen alleen verwerkt worden voor het doel waarvoor ze verzameld zijn. Als e-mailadressen verzameld worden om de leden op de hoogte te houden van welke wedstrijden er plaats zullen vinden, mogen deze niet gebruikt worden om reclame van bedrijven op te sturen.

   Daarnaast moet elke verwerking een juiste grondslag hebben (zoals hierboven kort benoemd). Een voetbalclub die al zijn informatie digitaal verstrekt, mag niet de fysieke adressen van leden verzamelen (tenzij hier een andere grondslag voor is natuurlijk). Voor verenigingen zal de grondslag voor hun gegevensverwerkingen voornamelijk de uitvoer van de lidmaatschapsovereenkomst zijn.

   Gegevens mogen niet langer bewaard worden dan noodzakelijk. Voor persoonsgegevens van een uitgetreden lid geldt bijvoorbeeld dat deze niet langer dan twee jaar bewaard mogen worden. Een uitzondering hierop is de fiscale bewaarplicht; gegevens die hier onder vallen *moeten* zeven jaar worden bewaard.

2. *Privacyverklaring en de rechten van betrokkenen*
   In de privacyverklaring (die aan de betrokkenen moet worden verstrekt, bijvoorbeeld via de website of het inschrijfformulier voor nieuwe leden) kunnen betrokkenen nalezen wat iemand gaat doen met hun persoonsgegevens en waarom, hoe deze worden beveiligd, wie er toegang tot heeft en hoe ze hun rechten onder de AVG kunnen uitvoeren. In vele blogs op internet is te lezen wat er précies in deze verklaringen moet staan.

   De betrokkene heeft een aantal rechten met betrekking tot hun persoonsgegevens: het recht om gegevens over te dragen naar een andere

partij, het recht om vergeten te worden, het recht op inzage, het recht op rectificatie en aanvulling van de gegevens, het recht op beperking van de verwerking, het recht met betrekking tot geautomatiseerde besluitvorming en profilering en het recht om bezwaar te maken tegen de gegevensverwerking. In principe moet er binnen één maand gereageerd worden op een verzoek op grond van één van deze rechten.

3. *Verwerkersovereenkomsten*
   Is een deel van de verwerkingen, bijvoorbeeld het bijhouden van een ledenbestand of personeelsadministratie, uitbesteed aan een derde partij (een verwerker), dan moeten er met deze partij afspraken gemaakt worden over deze doorgifte van gegevens. De AVG verplicht het om deze afspraken neer te leggen in een verwerkersovereenkomst. Deze regelt afspraken over beveiliging, de toegestane handelingen, controle van de verwerkingsverantwoordelijke (de vereniging) op de verwerker (de derde partij) en het uitbesteden van werk aan een sub-verwerker.

4. *Beveiliging*
   Afhankelijk van de gevoeligheid van de persoonsgegevens, moet er een passende beveiliging bestaan voor de opslag hiervan. Dit ziet ten eerste op de technische beveiliging (wachtwoorden, software die up-to-date is, etc.), maar heeft ook betrekking op de organisatorische beveiliging. Niet iedereen moet toegang kunnen krijgen tot computers met (gevoelige) persoonsgegevens. Leg vast wie de geautoriseerde medewerkers/vrijwilligers zijn.

5. *Beleid voor datalekken*
   Een datalek is een schending van de beveiliging waardoor persoonsgegevens in verkeerde handen zijn gevallen of kwijt zijn geraakt. Het kwijtraken van een USB-stick kan hier ook onder vallen. Een datalek moet gemeld worden aan de toezichthouder (de Autoriteit Persoonsgegevens) en de betrokkenen om wiens gegevens het gaat, tenzij het duidelijk is dat er geen of nauwelijks risico's zijn voor de privacy van de betrokkenen. Het melden moet binnen 72 uur gebeuren. Alle datalekken, ook de lekken die niet gemeld hoeven te worden, moeten intern geregistreerd worden, zodat deze op verzoek van de toezichthouder ingezien kunnen worden. Het is verstandig om een beleid op te stellen waarin vastgelegd wordt wat de te ondernemen stappen zijn in het geval van een datalek.

Tips voor verenigingen

6. *Het publiceren van de ledenlijst*
   Het publiceren van een ledenlijst op het internet door een vereniging is toegestaan mits de internetpagina is afgeschermd (bijvoorbeeld door een wachtwoord) en de verwerking is opgenomen in de doelstellingen van de vereniging. Op basis van oude jurisprudentie (niet zeker of dit zo zal blijven) hoeft géén expliciete toestemming aan leden gevraagd te worden als de ledenvergadering de publicatie heeft goedgekeurd. Beter: melden op het moment

van vastlegging. Een lid moet op verzoek zijn gegevens uit de ledenlijst kunnen laten halen.

7. *Het publiceren van beeldmateriaal*
   Als leden herkenbaar in beeld zijn gebracht, is het publiceren van dit beeldmateriaal aan regels gebonden. Ten eerste moet er toestemming van de betrokkene zijn. Deze toestemming moet ondubbelzinnig zijn; het moet duidelijk zijn voor welke verwerking en voor welk doel toestemming is gegeven. Dit kan er als volgt uitzien: "*Ik geef toestemming aan de vereniging om foto's van mij op voetbaltoernooien van onze vereniging te publiceren op hun facebookpagina"*. Voor kinderen onder de 16 jaar moeten de ouders deze toestemming geven. Deze toestemming kan ook weer ingetrokken worden, dan moeten de foto's verwijderd worden.

   Ten tweede moeten er passende technische en organisatorische beveiligingsmaatregelen getroffen worden om de foto's te beschermen. Zeker als er foto's van kinderen gepubliceerd worden, moeten deze goed beveiligd zijn tegen misbruik. Voorbeelden zijn een website die alleen toegankelijk is met een wachtwoord of een afgeschermde facebookpagina.

8. *Elektronische mailings*
   Een vereniging mag haar nieuwsbrief gewoon aan de leden versturen. Als er naast algemene clubinformatie ook commerciële boodschappen in zijn opgenomen, vraag dan toestemming aan betrokkene voor het versturen van de nieuwsbrief. Biedt in ieder geval een uitschrijfmogelijkheid aan in elke nieuwsbrief.

9. *Het delen van NAW-gegevens en e-mailadressen*
   Het doorgeven van NAW-gegevens aan bijvoorbeeld sponsoren is alleen toegestaan met de uitdrukkelijke toestemming van een lid. Het versturen van reclame per post kan echter ook in algemene zin door de ledenvergadering goedgekeurd worden. Of leden dergelijke post kunnen ontvangen, moet wel met ze gecommuniceerd worden en ze moeten zich hiertegen kunnen verzetten.

   Voor het versturen van commerciële berichten via de e-mail kan er geen algemene toestemming door de ledenvergadering worden gegeven. Een sponsor zal dan de uitdrukkelijke toestemming van individuele ontvangers moeten verkrijgen voordat verenigingen de e-mailadressen van leden aan hen kunnen verstrekken.

10. *Verhouding met koepelorganisaties*
    Als een koepelorganisatie ook gegevens van leden ontvangt, moet er goed gekeken worden naar de rolverdeling tussen de vereniging en de koepelorganisatie. Vaak is de koepelorganisatie óók verwerkingsverantwoordelijke, en zullen er afspraken gemaakt moeten worden over de verdeling van verantwoordelijkheden en plichten ten opzichte van de betrokkenen. Het is verstandig om met de koepelorganisatie te bespreken of dit inderdaad nodig is.