AVG

Algemeen

Voor het verkrijgen van een AVG verklaring moet de vereniging voldoen aan een aantal eisen. Bij de invulling tot verkrijging is al geanticipeerd op deze voorwaarden. Voor 25 mei moeten we de vereisten wel geïmplementeerd hebben. In de volgende passages worden de voornaamste voorwaarden beschreven en geven we in de kaders aan wat we nog moeten doen voor 25 mei. Het moge duidelijk zijn dat hier geen sprake is van een vrijwillige keuze, maar van een wettelijke verplichting die, bij niet naleven, kan/zal leiden tot onaangename boetes.

Inventarisatie persoonsgegevens

De wet maakt onderscheid in gevoelige gegevens en bijzondere gegevens. voor gevoelige gegevens is geen algemeen verbod, voor bijzondere gegevens wel.

Gewone persoonsgegevens	Bijzondere persoonsgegevens
☐ Naam/ voorletters/ tussenvoegsel ☐ Titels ☐ Adres ☐ Postcode ☐ Plaats ☐ Provincie ☐ Land ☐ Woonplaats ☐ Telefoonnummer ☐ Faxnummer ☐ E-mailadres ☐ Website ☐ Geslacht ☐ Geboortedatum ☐ Geboorteplaats ☐ Overlijdensdatum ☐ Burgerlijke staat ☐ LinkedIn ☐ Facebook ☐ Twitter ☐ Werkzaam bij organisatie ☐ Bankrekeningnummer	☐ Etnische afkomst ☐ Politieke opvattingen of voorkeur ☐ Religieuze opvatting of overtuiging ☐ Lidmaatschap van een vakbond ☐ Genetische of biometrische gegevens met het oog op unieke identificatie ☐ Gegevens over gezondheid ☐ Gegevens over seksuele geaardheid ☐ Strafrechtelijke gegevens of veroordelingen of daarmee verband houdende veiligheidsmaatregelen ☐ Salarisgegevens ☐ Paspoort kopie, waarop pasfoto zichtbaar is (zonder voorlegger gekopieerd) ☐ BSN-nummer ☐ Handicap classificatie code Het registreren van deze bijzondere gegevens is toegestaan: - Na toestemming van betrokkene - Openbaarmaking van betrokkene op bvb zijn site - Indien juridisch noodzakelijk - Als dat van vitaal belang is Hiervoor is dan wel een voorakkoord getekende verklaring noodzakelijk.

☐ Inloggegevens (gebruikersnaam/wachtwoord) ☐ Voertuig kentekenplaat ☐ Tak van sport ☐ Lidmaatschapsnummer ☐ Wedstrijdnummer/startnummer ☐ Opleiding/beroep ☐ Sport specifieke diploma's	

De meeste van de gegevens die wij registreren zijn gevoelige gegevens. Onder bijzondere gegevens die wij wel eens opslaan zijn te rekenen:

- Gegevens over gezondheid; in bijzondere gevallen vanwege gezondheidsrisico's zoals hart of longproblemen of vanwege recente blessures (in een herstelperiode) moeten we deze gegevens noteren. Dat is een aanvaarde reden voor de AVG
- Het in bezit hebben van een kopie paspoort en/of BSN nummer
  Onbekend is of dit soort legitimaties bij de ledenadministratie bewaard worden. Een BSN nummer is alleen nodig als er sprake is van uitbetaling van salarissen of vergoedingen. In alle andere gevallen lijken paspoorten en BSN nummers niet noodzakelijk en zullen we die moeten vernietigen.

Vernietigen van bijzondere gegevens zoals kopieën van paspoorten en BSN nummers als die niet strikt noodzakelijk zijn voor het nakomen van wettelijke verplichtingen.

Er moet zekerheid zijn dat alle persoonsgegeven in beeld zijn. Daarom moeten we de volgende stappen doorlopen:

- Controleer alle computerapplicaties en vink de gevonden persoonsgegevens aan op een checklist;
- Controleer ook persoonsgegevens die je als vereniging hebt ondergebracht bij derde partijen, b.v. een salarisadministratiekantoor;
- Controleer elektronische documenten (Excel-lijstjes, Word-documenten, etc.) en vink de gevonden persoonsgegevens aan op een checklist;
- Controleer alle papieren documenten (denk ook aan kopieën van een paspoort of rijbewijs) en vink de gevonden persoonsgegevens aan op de checklist

Op een aanmeldingsformulier voor het lidmaatschap altijd vermelden dat de vermelde gegevens voor verenigingsdoeleinden gebruik mogen worden en dat betrokkenen dit gelezen heeft en akkoord is.Als extra slot op de deur bovendien:

Gegevens worden gebruikt in overeenstemming met de privacyregels

Alle gegevens mogen gebruikt worden voor het organiseren van wedstrijden, activiteiten en evenementen waarbij de vereniging is betrokken

De maximale bewaartermijn van de gegevens is de duur van het lidmaatschap plus 2 jaar daarna, tenzij anders schriftelijk wordt overeengekomen

Het maken en gebruiken van vrijwilligersovereenkomst met daarin deze privacy policy.

Leg voor de vereniging een register aan waarin vermeld
alle gegevens
De reden waarom deze worden bewaard
De wettelijke grondslag
De bewaartermijn
Beveiliging

Persoonsgegeven mogen maar een beperkte tijd worden bewaard. De wet schept een belangrijke uitzondering om persoonsgegevens langer te mogen bewaren dan noodzakelijk is voor het doel waarvoor ze oorspronkelijk zijn verkregen of verwerkt. Je mag persoonsgegevens namelijk langer bewaren als daarmee een historisch, statistisch of wetenschappelijk doel is gediend. Je moet wel zorgen dat de persoonsgegevens niet alsnog zomaar voor andere doeleinden uit het archief kunnen worden gehaald. De begrippen 'historisch', 'statistisch' en 'wetenschappelijk' zijn nogal algemeen. Het is in de praktijk dan ook niet altijd duidelijk wat hier nu precies wel of niet onder valt. Om je op weg te helpen geven we drie voorbeelden waarin deze uitzonderingsgrond behulpzaam kan zijn.

Voorbeeld: clubhistorie Verenigingen hechten er meestal waarde aan om een bepaald erfgoed van de club op te bouwen. Denk aan sportprestaties of fotomateriaal. Dat is in principe geen probleem, maar zorg dan wel dat er geen onnodige gegevens in de archieven belanden. Bovendien moet je voorkomen dat persoonsgegevens uit het archief later alsnog voor andere dan historische doeleinden worden gebruikt.

Voorbeeld: statistiek Het kan voor een organisatie om allerlei redenen prettig zijn om bepaalde persoonsgegevens voor statistische doeleinden langer te bewaren. Dat is doorgaans geen probleem. Stel dan wel duidelijk vast welke persoonsgegevens daarvoor wel en niet noodzakelijk zijn, en voorkom ook hier dat jij of een derde de langer bewaarde gegevens alsnog voor andere doeleinden gaat gebruiken. Overweeg ook of het mogelijk is om de gegevens te anonimiseren of pseudonimiseren, zodat je de negatieve invloed op iemands privacy wegneemt of beperkt.

Voorbeeld: wetenschappelijk onderzoek Het bijhouden van sport gerelateerde data resulteert vaak in bergen informatie die niet alleen interessant zijn voor de sporter en sportorganisaties, maar ook voor de wetenschap. Denk bijvoorbeeld aan medisch-wetenschappelijk onderzoek. Het is in principe toegestaan om dit soort persoonsgegevens om die reden langer te bewaren. Hier geldt overigens wel dat het vaak om gezondheidsgegevens gaat. Het is daarom extra belangrijk dat je overweegt ook of het mogelijk is om de gegevens te anonimiseren of pseudonimiseren, zodat je de negatieve invloed op iemands privacy wegneemt of beperkt.

Wil je bepaalde persoonsgegevens op enig moment voor andere doeleinden gaan gebruiken, stel dan altijd de volgende vragen:

1. Bestaat er voldoende samenhang tussen het oorspronkelijke en nieuwe ‘doel’ waarvoor je de persoonsgegevens wil gebruiken? Onthoud daarbij dat wanneer de verwantschap tussen deze doelen kleiner is, er minder kans bestaat dat je de persoonsgegevens kunt ‘hergebruiken’.
2. Zijn de gegevens niet te gevoelig om voor alternatieve doeleinden te gebruiken dan waarvoor ze oorspronkelijk zijn verkregen?

3. Kan worden uitgesloten dat er nadelige gevolgen voor de betrokkene zijn als ik de persoonsgegevens ga gebruiken voor het alternatieve doel?
4. Is er voldoende gelegenheid om de betrokkene te informeren over het nieuwe doel, zodat een onwenselijk verrassingseffect achterwege blijft?

Is het antwoord op deze vragen hoofdzakelijk ontkennend, dan kan je vermoeden dat het alternatieve gebruik niet verenigbaar is met het doel waarvoor je de persoonsgegevens hebt verkregen.

De privacy policy van de vereniging moet voor iedereen vindbaar zijn. Het eenvoudigste is om deze op de website van de vereniging te zetten en op elke pagina (onderaan) een link hier naar toe te leggen.
In alle overeenkomsten (documenten waarin persoonsgegevens gevraagd worden) moet een verwijzing staan naar de privacy policy.

Werken met verwerkersovereenkomst

De vereniging moet er voor zorgen dat andere partijen/relaties geen gebruik maken van aan de vereniging toevertrouwde persoonsgegeven. Daarom moet er met iedere relatie die persoonsgegevens van de vereniging gebruikt een verwerkingsovereenkomst afgesloten worden.

De vereniging mag nooit persoonsgegevens doorgeven aan andere partijen waarmee er geen verwerkersovereenkomst is afgesloten. als dit noodzakelijk is voor uitvoering van de doeleinden waarvoor we ze hebben gekregen. Een model verwerkingsovereenkomst is als apart document toegevoegd.

Toegankelijkheid

In de vereniging hebben alleen geautoriseerde personen toegang tot de persoonsgegevens van de vereniging ter voorkoming van datalekken. Er worden 4 autorisaties uitgeschreven voor een ledenbestand van (geschat) 450 personen

Vernietiging persoonsgegevens

Indien er geen grondslag meer is waarop bepaalde persoonsgegevens zijn verwerkt, dienen deze persoonsgegevens (al dan niet met inachtneming van een bewaartermijn) te worden verwijderd. Bij vernietigen moet nagegaan worden waar de gegevens van een persoon gebruikt kunnen zijn, zoals:
- de ledenlijst die in een Excel-bestand bewaard wordt op het netwerk;
- een telefoonnummer in een mobiele telefoon;
- mailtjes in een mailbox;
- een los documentje op een laptop;
- een registratie in een CRM-systeem met daaraan vele gekoppelde gegevens;
- een bestand bij de drukker voor het verzenden van het verenigingsblad;
- en nog veel meer…

Let op: In de financiële administratie moeten deze persoonsgegevens nog wel blijven staan, want daar geldt een (wettelijke) bewaarplicht van 7 jaar.

Genomen beveiligingsmaatregelen en bewustwording

Als vereniging zorg je voor technische en organisatorische beveiligingsmaatregelen om een beveiligingsniveau te bereiken dat past bij het risico. Het gaat om gegevens die uit privacy-oogpunt extra aandacht behoeven. Hierbij houd je rekening met de laatste stand van de techniek, de kosten van implementatie, evenals de aard, de reikwijdte, de context, de doeleinden van de verwerking en de risico's voor de rechten en vrijheden van personen. Daarbij moet je de volgende, passende maatregelen nemen.

- Alle persoonsgegevens zijn alleen te bereiken via een inlog, dit kan zijn een wachtwoord op een telefoon of een usernaam en wachtwoord op een computer;
- Gebruik zo veel mogelijk versleutelde gegevensdragers als je bijzondere persoonsgegevens moet vervoeren. Hiermee zorg je ervoor dat de persoonsgegevens voor anderen niet leesbaar zijn;
- Gebruik beveiliging op netwerkmappen en waar nodig ook beveiliging op bestanden op het netwerk;
- Overweeg om meervoudige authenticatie in te voeren (naast een gebruikersnaam en een wachtwoord moet dan ook een code ingevoerd worden, die je bijvoorbeeld via SMS ontvangt);
- Sluit de website/het netwerk af voor landen waarvoor dit niet strik noodzakelijk is. Toelichting: het is mogelijk om internetverkeer naar de vereniging af te sluiten voor landen waar vandaan veel hackers actief zijn. Werk hierbij van binnen naar buiten, dus alleen openstellen voor landen waarvoor dat stikt noodzakelijk is;
- Als persoonsgegevens via een besloten website te benaderen zijn, moet die beveiligde internetverbinding te herkennen zijn aan het groene slotje (HTTPS);
- Als je bijzondere persoonsgegevens in je CRM opgeslagen hebt, zorg er dan voor dat deze alleen door de juiste personen (met autorisatie) te zien zijn;
- Laat alle medewerkers een geheimhoudingsverklaring tekenen, zodat men zich bewust is van de risico's en hun rol daarin;
- Zorg voor een goede back-up procedure met onder andere een regelmatige test van het herstellen van de gegevens;
- Test en evalueer regelmatig de maatregelen en de beveiliging.

Wat je verder moet doen

1. Zorg ervoor dat alle medewerkers van je vereniging op de hoogte zijn van AVG, de eisen en verplichtingen en laat ze een geheimhoudingsverklaring (toegevoegd als apart document) tekenen;
2. Bewaar alle gegevens altijd achter een wachtwoord of sleutel (computer, laptop, telefoon of beveiligde USB);
3. Verander tijdig je wachtwoord;
4. Houd software en virusscanners altijd up-to-date;
5. Maak periodiek back-ups van de gegevensbestanden zodat de persoonsgegevens beschermd zijn tegen verlies bij incidenten;
6. Gebruik bij voorkeur geen USB-sticks en áls het moet alleen versleutelde sticks als daar persoonsgegevens op staan.

Mobiele telefoon

Als je persoonsgegevens, zoals bijvoorbeeld telefoonnummers, opslaat op een mobiele telefoon, zorg er dan voor dat er altijd een wachtwoord of een codebeveiliging aanstaat op deze telefoon.

Toegangsbeveiliging

Om zeker te weten dat alleen geautoriseerde personen de persoonsgegevens kunnen inzien en bewerken, moeten deze altijd beveiligd zijn met een wachtwoord en als het kan ook met een gebruikersnaam. Zo kun je een Excel-bestand beveiligen met een wachtwoord en een PC voorzien van een gebruikersnaam en een wachtwoord. Zorg er dus voor dat je altijd minimaal één keer een wachtwoord moet weten voordat je de persoonsgegevens van jouw vereniging gaat inzien of bewerken.

Als je gebruik maakt van bijzondere persoonsgegevens, zorg dan extra goed voor de toegangsbeveiliging. Hierbij ga je eerst goed in kaart brengen welke bijzondere persoonsgegevens je hebt en wie er geautoriseerd is om deze te mogen verwerken.

Zorg er minimaal voor dat deze gegevens beveiligd zijn met een gebruikersnaam en een wachtwoord. Als de vereniging gebruikt maakt van bijzondere persoonsgegevens is het aan te raden om één of meerdere van onderstaande maatregelen ook te treffen:
- wachtwoord regelmatig wijzigen;
- een tweede autorisatiemethode toepassen zoals een extra code via SMS;
- automatische schermblokkering na 3 minuten van inactiviteit;
- afsluiten van ruimtes waar deze gegevens verwerkt worden;
- geen gasten op het WIFI netwerk.

DUS: Hoe gevoeliger de bijzondere persoonsgegevens zijn, des te beter moeten de maatregelen zijn.

Publicatie op internet

Niemand mag zomaar persoonsgegevens (dus ook geen foto) van een ander op internet publiceren. Dit mag in principe alleen als deze persoon hiervoor toestemming geeft. Mensen hebben ook het recht om hun toestemming later in te trekken. Dat geldt dus ook voor verenigingen, ook al plaatsen mensen gegevens zelf op het internet, zoals op Facebook of LinkedIn. Reden om hier streng op te zijn: eenmaal op internet geplaatste gegevens kunnen jaren later nog vindbaar zijn en negatief zijn voor betrokkenen, bijvoorbeeld bij een sollicitatie.

Toestemming bij kinderen

Bij het aanmelden bij de vereniging in geval van kinderen jonger dan 16 jaar, is extra aandacht vereist. In dat geval moet getekend worden door de ouder/verzorger.

Maar de verplichting geldt ook voor:
- aanmelden voor een nieuwsbrief;
- inschrijven voor een bijeenkomst;
- aanmelden voor een uitstapje.

Worden ook dit soort aanmeldingen/inschrijvingen gebruikt, dan moet je ook daar controleren op toestemming bij kinderen. Zorg dus dat je bij kinderen altijd vraagt om toestemming.

Als je persoonsgegevens hebt van personen jonger dan 16 jaar, dan moet je daarvoor altijd schriftelijk een handtekening (op papier!) voor akkoord hebben van de ouder, verzorger of wettelijke vertegenwoordiger. Geef hier onder aan dat je vereniging dat ook altijd zo doet.

AVG-dossier

Via e-mail is er een AVG-verklaring aangevraagd en ontvangen. Deze is onderdeel van het AVG-dossier van de vereniging. Er wordt een map aangelegd met onderstaande indelingen en die wordt gevuld/onderhouden zoals hieronder beschreven is.

AVG-dossier

1. AVG-verklaring;
2. Inventarisatie:
    - matrix persoonsgegevens;
    - matrix verwerkingen, persoonsgegevens, doel, overeenkomst, bewaartermijn;
3. Privacy policy;
4. Verwerkersovereenkomsten met leveranciers;
5. Geheimhoudingsverklaringen van medewerkers;
6. Overeenkomsten:
    - Lidmaatschapsovereenkomsten;
7. Datalekken rapportages;
8. AVG-gerelateerde procedures:
    - back-up;
    - verwijderen;
    - sleutelbeleid;
9. Verwerkingenregister
    - type persoonsgegevens;
    - de verwerkingsdoeleinden;
    - bron van de gegevens;
    - met welke partijen worden gegevens gedeeld;
    - bewaartermijn;