Dossier: Hoe maak je jouw organisatie AVG-bestendig? Een 7-stappenplan

Op 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing voor alle organisaties die gegevens van personen (persoonsgegevens) in een bestand bewaren. Deze organisaties moeten zich aan de regels in deze nieuwe verordening houden. Dat geldt zowel voor het bewaren in digitale bestanden als in mappen op een plank. Ook deze laatste moeten voortaan veilig worden opgeborgen zonder dat vreemden daar bij kunnen. Met onderstaande zeven stappen maak je jouw organisatie AVG-bestendig!

Stap 1: Ga waarom, hoe en wat na

Ga na welke persoonsgegeven worden verzameld en waar die worden bewaard. In de nieuwe AVG zijn ook vrijwilligersorganisaties verplicht te inventariseren wat ze vastleggen én te registreren welke persoonsgegevens ze hoe vastleggen. Ook moeten ze bedenken of dat wat ze opslaan wel functioneel is; waarom leggen ze welke gegevens vast. Dit houdt in dat je alleen persoonsgegevens vastlegt die je nodig hebt en dat je ze alleen gebruikt waarvoor je ze verzamelt.

Denk bijvoorbeeld aan de voetbalvereniging die standaardadressen (straatnaam, postcode, huisnummer) van de leden in een bestand bewaard terwijl alle communicatie per telefoon, sociale media en digitale nieuwsbrief gaat. Deze clubs hoeven helemaal geen straat en huisnummer te bewaren. Het zal even wennen zijn maar hoe minder informatie er over personen bewaard wordt, hoe moeilijker gegevens herleidbaar zijn naar een persoon en hoe minder kans op schending van de privacy.

Stap 2: Laat weten wat je bewaart

Onveranderd maar wel van belang is dat betrokkenen toestemming geven voor het gebruik van hun persoonsgegevens. Alleen wanneer daar een dringende reden van algemeen belang of wetgeving voor is, kunnen persoonsgegevens zonder toestemming worden opgeslagen. Nieuw is dat de betrokkenen moet weten dat zijn persoonsgegevens worden verwerkt en met welk doel. Zijn hebben het recht hun gegevens in te zien en aan te (laten) passen. Bij verenigingen is helder dat persoonsgegevens noodzakelijk zijn voor het lidmaatschap en om deel te nemen aan de activiteiten. Dit laatste geldt ook voor deelname aan activiteiten van een stichting.

Pas op met bijzondere persoonsgegevens

Verwerken van bijzondere persoonsgegevens is verboden, tenzij hiervoor een wettelijke uitzondering is of de persoon daar uitdrukkelijk tostemming voor heeft gegeven. Dit zijn persoonsgegevens van gevoelige aard zoals godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, lidmaatschap van een vakvereniging of politieke partij, strafrechtelijke persoonsgegevens en persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd verbod naar aanleiding van dat gedrag, genetische en biometrische kenmerken. Onder deze laatste vallen vingerafdrukken, stem, handschrift, geometrie van de handomtrek en scans van netvlies, iris en gelaat.

Ook medische informatie, bijvoorbeeld over diabetes of allergieën, mag je alleen opslaan als er een wettelijke uitzondering is. Organisaties hebben nu de neiging deze informatie automatisch op te slaan in een bestand. Dat is niet langer toegestaan. Deze informatie moet dus iedere keer gevraagd voor activiteiten waarbij dat van belang is.

Stap 3: Vastleggen hoe de organisatie met de data omgaat

Organisaties hebben een verantwoordingsplicht in de nieuwe AVG. Dat betekent dat organisaties vastleggen wie verantwoordelijk is voor de data, aan wie informatie wordt verstrekt en ook op welke computer deze wordt opgeslagen en op welke wijze deze wordt beschermd tegen virussen en hacken.

Niet onbelangrijk; zorg dat de data maar op één computer of één systeem staan. Verspreiding van data over verschillende computers of systemen zonder dat dat is vastgelegd kan uitgelegd worden als datalekken.

Er moeten procedures worden opgesteld om personen toegang te geven tot de informatie. Met externe gebruikers van de bestanden, zoals drukkers, verspreiders van de nieuwsbrieven en bijvoorbeeld de koepelorganisatie, moeten overeenkomsten worden opgesteld voor het gebruik van gegevens; de zogenoemde verwerkersovereenkomst. In deze overeenkomsten moeten bijvoorbeeld ook afspraken gemaakt worden over het vernietigen van de gegevens na gebruik. Ook wanneer het om de koepelorganisatie gaat, moeten afspraken gemaakt worden over het gebruik van de bestanden. De organisaties maken immers afspraken met de leden over het zorgvuldig bewaren van hun gegevens en daar kan een organisatie op aangesproken worden.

Stap 4: Stel zo nodig een functionaris voor de gegevensbescherming (FG) aan

Dit is niet verplicht voor alle organisaties. Wel voor overheids- en publieke organisaties, organisaties die persoonsgegevens analyseren (profiling) en wanneer bijzondere persoonsgegevens worden opgeslagen. Voor organisaties waarvoor een FG niet verplicht is, kan het wel handig zijn een FG aan te stellen. De FG is de centrale persoon die alle persoonsgegevens van de club beheert. Deze FG heeft zeggenschap over de bestanden en legt verantwoording af aan de verantwoordelijke beheerder, meestal het bestuur. Deze persoon beslist in opdracht van het bestuur over hoe bestanden worden opgeslagen en de procedure voor het beschikbaar stellen van de gegevens. Ook bestuursleden kunnen alleen via van tevoren vastgelegde procedures gegevens gebruiken. De FG zorgt er ook voor dat de virusscan op orde is en dat de computer beschermd is tegen hacken.

Voor organisaties die verplicht een Functionaris Gegevensbescherming (FG) moeten aanstellen heeft deze formeel de volgende verplichting:

- FG's mogen alleen handelen in opdracht van de verantwoordelijke;
- FG's worden verplicht een overzicht bij te houden van alle categorieën persoonsgegevens die zij verwerken in opdracht van en verantwoordelijke;
- FG's moeten passende technische en organisatorische beveiligingsmaatregelen nemen die een passend beschermingsniveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen. FG's moeten uitgebreide kennis hebben omtrent hun informatiesystemen en de typen data die zij verwerken (is er sprake van bijzondere persoonsgegevens?);
- FG's mogen geen sub-FG's inschakelen zonder toestemming van de verantwoordelijke, wanneer sub-FG's worden ingezet moet de FG de nodige technische en organisatorische maatregelen nemen om de veiligheid en integriteit van de data te garanderen;
- FG's moeten de verantwoordelijke onmiddellijk op de hoogte stellen van een datalek. De termijn voor 'onverwijld' in de Nederlandse wetgeving wordt in de Wet Meldplicht datalekken vastgesteld op 72 uur na ontdekking van het incident;
- FG's zijn verplicht medewerking te verlenen aan verzoeken van de Autoriteit Persoonsgegevens;
- In bepaalde gevallen moet de FG een Privacy Impact Assessment uitvoeren. Dat is in ieder geval zo bij profiling, het verwerken van bijzondere persoonskenmerken en opslaan van camerabeelden met personen erop.

Stap 5: Privacy Impact Assessment (PIA)

Hiermee breng je in beeld wat de gevolgen zijn van het verzamelen van persoonsgegevens voor de personen zelf. Dit is afhankelijk van wat met de gegevens gedaan wordt. Wanneer de gegevens verzameld worden voor het versturen van de contributiebrief of een nieuwsbrief is het effect dat mensen lid blijven van de organisatie of dat ze geïnformeerd zijn over de organisatie. Niet voor alle bestanden met persoonsgegevens hoeft daarom een PIA gedaan te worden. Alleen wanneer:

- Met de persoonsgegevens systematisch persoonlijke aspecten worden geëvalueerd (profiling)
- Op grote schaal bijzondere gegevens worden verwerkt (zie stap 1)
- Personen gevolgd worden in publieke ruimte (b.v. door cameratoezicht)

Voor de meeste vrijwilligersorganisaties is een formele PIA niet nodig. Vooral niet omdat alleen contactgegevens verzameld worden en geen persoonskenmerken.

Stap 6: Vrijwilligers informeren of opleiden

Het is niet de bedoeling dat wanneer je de gegevensbescherming zorgvuldig in beleid en procedures hebt geregeld, de eerste de beste vrijwilliger met persoonsgegevens die nodig zijn bij de uitoefening van de zijn/haar functie, te koop gaat lopen. Ook dat zijn datalekken. Dit kan gaan om gegevens uit de bestanden van de organisatie zelf, maar ook om informatie die een vrijwilliger van een deelnemer of ouder heeft gekregen.

Stap 7: Procedure opstellen voor het melden van datalekken

Elke organisatie die persoonsgegevens opslaat, is verplicht datalekken te melden binnen 72 uur na ontdekking. Om dit zorgvuldig te doen is het handig vooraf procedures af te spreken. Hierin staat:

- Wat een datalek is;
  We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Een datalek is het gevolg van een beveiligingsprobleem. In de meeste gevallen gaat het om uitgelekte computerbestanden, een gestolen geprinte ledenlijst of cliëntgegevens. Andere voorbeelden zijn cyberaanvallen, verkeerd verzonden e-mail, gestolen laptops, afgedankte niet-schoongemaakte computers en verloren usb-sticks.
- Bij wie in de organisatie een datalek gemeld moet worden;
- Wie binnen de organisatie 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 persoon 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 persoonsgegevens;
  - De maatregelen die de organisatie heeft genomen of voorstelt te nemen om deze gevolgen te verhelpen.
- Wie de melding doet bij de Autoriteit Persoonsgegevens.

Meldingen kunnen digitaal gedaan worden bij het meldloket van de Autoriteit Persoonsgegevens: http://datalekken.autoriteitpersoonsgegevens.nl

Wie controleert?

In Nederland controleert de Autoriteit Persoonsgegevens of organisaties voldoen aan de Algemene Verordening Gegevensbescherming. De Autoriteit Persoonsgegevens kan ook boetes opleggen wanneer na waarschuwingen een organisatie het beleid rond bescherming persoonsgegevens niet verbetert

Wat betekent de AVG voor jouw vereniging?

Posted on 19 maart 2018 by Puck Geytenbeek

Deze blog is bedoeld om je in te lichten over de Algemene Verordening Gegevensbescherming (AVG) en je bewust te maken van de impact op jouw vereniging.

Je leest het al in de eerste zin van deze blog; bewustwording is belangrijk voor de AVG! Wees je er als vereniging van bewust dat je dagelijks te maken hebt met de persoonsgegevens van je leden. Jouw leden gaan er vanuit dat je met zorg omgaat met hun persoonsgegevens. Het is belangrijk dat iedereen binnen de vereniging die betrokken is bij het verwerken van de persoonsgegevens weet wat de AVG inhoudt.

In deze blog lees je wat de AVG inhoudt, welke impact dat op jouw vereniging heeft en bieden we je een stappenplan om je vereniging en Congressus zo in te richten dat je kan voldoen aan de AVG.

Liever offline lezen? Download hier de volledige blog

Disclaimer
Deze blog is door Congressus samengesteld om je vereniging zo goed mogelijk op de hoogte te brengen van de AVG en de impact hiervan op je vereniging. We kunnen echter niet garanderen dat deze blog alles omvattend danwel volledig juist is.

Wat is de AVG?

De AVG, of de Engelse benaming ‘GDPR’, bevat nieuwe privacy-wetgeving die voor heel Europa gelijk is. De AVG vervangt hiermee de oude landelijke wetgeving (in Nederland de Wet Bescherming persoonsgegevens) en zorgt ervoor dat de regels rondom privacy en persoonsgegevens overal in Europa hetzelfde zijn. Vanaf 25 mei 2018 is de AVG van kracht en handhaaft de Autoriteit Persoonsgegevens, de Nederlandse toezichthouder, deze nieuwe privacywet. Indien na controle blijkt dat je niet voldoet aan de AVG kan je een boete verwachten. Deze boete kan oplopen tot €20.000.000 of 4% van de jaaromzet.

Elke organisatie verwerkt persoonsgegevens zoals namen, adressen en telefoonnummers. Het belangrijk dat je daar zorgvuldig mee omgaat. Het is bijvoorbeeld vereist om toestemming te hebben voor de verwerking van persoonsgegevens voordat je deze verwerkt. Met ingang van de AVG worden deze regels nog strenger.

De AVG is een inspanningswet, dat betekent dat je moet kunnen aantonen dat je alles hebt gedaan wat binnen je macht ligt om aan de AVG te kunnen voldoen. Er wordt dan ook van je verwacht dat je actief aan de slag gaat en stappen neemt. Je zult dus van alles moeten uitzoeken, aanpassen en vastleggen. Zorg dat je hier tijdig mee begint!

De AVG in het kort:

- Je moet precies weten welke persoonsgegevens je verwerkt en beheert
- Je moet weten welke rechten de personen hebben van wie je de persoonsgegevens verwerkt en bezit
- In je dienst moet je rekening houden met privacy by design en privacy by default
- Projecten met hoog risico op een (data)lek moeten vooraf een inschatting van het privacyrisico krijgen; een Privacy Impact Analyse (PIA)
- Je mag persoonsgegevens alleen maar gebruiken voor het doel waarvoor je de persoonsgegevens hebt ontvangen

Op de website van Autoriteit Persoonsgegevens kun je alles over de AVG lezen. Wil je de volledig wet downloaden, dan kan dat hier.

Wat betekent de AVG voor jouw vereniging?

In dit hoofdstuk lichten we enkele aspecten van de AVG toe die relevant zijn voor jouw vereniging.

Rechten van de betrokkenen

Als vereniging zorg je ervoor dat je leden hun rechten met betrekking tot hun persoonsgegevens goed kunnen uitoefenen. Je leden hebben de volgende rechten:

1. **Recht op inzage**
   Indien een lid vraagt om inzage moet je het lid kunnen laten weten:
   - of je zijn persoonsgegevens gebruik en zo ja, om welke gegevens het gaat;
   - wat het doel is van het gebruik;
   - aan wie je de gegevens nog meer hebt verstrekt;
   - wat de herkomst van de gegevens is (indien de herkomst bekend is).
2. **Recht op correctie en verwijdering**
   Een lid mag een correctie aanvragen als:
   - zijn persoonsgegevens feitelijk onjuist zijn;
   - de persoonsgegevens van het lid onvolledig zijn of niet ter zake doen voor het doel waarvoor ze zijn verzameld;
   - zijn persoonsgegevens op een of andere manier in strijd met de wet worden gebruikt.
3. **Recht om vergeten te worden**
   Het lid heeft het recht om te eisen dat de vereniging de verwijdering doorgeeft aan alle

organisaties die deze gegevens van de vereniging hebben gekregen. Je moet vervolgens ook aan het lid kunnen bewijzen dat deze gegevens verwijderd zijn. Dit recht is niet ‘absoluut’. Zo kun je bijvoorbeeld eisen dat leden eerst al hun schulden aan de vereniging voldoen, voordat je alle persoonsgegevens van het lid verwijderd.

4. **Recht op dataportabiliteit**
   Je leden hebben het recht om (onder bepaalde voorwaarden) hun persoonsgegevens in een standaard formaat op te vragen. Voor dit standaard formaat zou je bijvoorbeeld gebruik kunnen maken van een export naar Excel.

Verwerkingsregister

Omdat bij verenigingen de verwerking van persoonsgegevens over het algemeen structureel is, is het verplicht om een verwerkingsregister bij te houden.

Wat moet je in het verwerkingsregister bijhouden?
Wat er in het verwerkingsregister moet staan, is afhankelijk van of je de verwerkingsverantwoordelijke of de verwerker bent. Als vereniging bepaal je zelf het doel en de middelen voor de verwerking van persoonsgegevens waardoor je de verwerkingsverantwoordelijke bent. Congressus is bijvoorbeeld verwerker van jullie persoonsgegevens.

Volgens de wet moet de verwerkingsverantwoordelijke de volgende informatie in het register opnemen:

1. de naam en contactgegevens van:
   - de vereniging, of de vertegenwoordiger van de vereniging;
   - eventuele andere organisaties met wie je gezamenlijk de doelen en middelen van de verwerking hebt vastgesteld;
   - de Functionaris voor de gegevensbescherming (FG) als je die hebt aangesteld;
   - eventuele andere internationale organisaties waar je persoonsgegevens mee deelt.
2. de doelen waarvoor je de persoonsgegevens verwerkt. Bijvoorbeeld voor de werving en selectie van personeel, het bezorgen van producten, direct marketing, het bijhouden van de ledenadministratie, de verkoop en levering van producten, het versturen van nieuwsbrieven en het versturen van uitnodigingen;
3. een beschrijving van de categorieën van personen van wie je gegevens verwerkt. Bijvoorbeeld leden, donateurs, alumni;
4. een beschrijving van de categorieën van persoonsgegevens. Zoals het BSN, NAW-gegevens, telefoonnummers, IP-adressen;
5. de periode waarna je de gegevens moet verwijderen (als dit bekend is);
6. de categorieën van ontvangers aan wie je persoonsgegevens verstrekt;
7. deel je de gegevens met een land of internationale organisatie buiten de EU? Dan moet je dit aangeven in het register;
8. een algemene beschrijving van de technische en organisatorische maatregelen die je hebt genomen om persoonsgegevens die je verwerkt te beveiligen.

Privacy by design en Privacy by default

Privacy by design betekent dat je er voor zorgt dat persoonsgegevens goed worden beschermd. Maar ook dat je niet meer gegevens verzamelt dan noodzakelijk voor het

doel van de verwerking én dat je deze gegevens niet langer bewaart dan noodzakelijk is.

Privacy by default betekent dat je technische en organisatorische maatregelen moet nemen om ervoor te zorgen dat de je alleen persoonsgegevens verwerkt die noodzakelijk zijn voor het specifieke doel dat je wilt bereiken.

Dit betekent dat je als vereniging goed moet nadenken over de persoonsgegevens die je van je leden bewaart. Stel jezelf de volgende vragen:

- Met welk doel verwerk je de persoonsgegevens?
- Zijn al deze gegevens noodzakelijk om lid te zijn van je vereniging?
- Hoe lang heb je de persoonsgegevens nodig?
- Wat is het beleid van jouw vereniging hierin?

Toestemming

De AVG stelt strengere eisen aan de toestemming van betrokkenen. Je zult dus moeten registreren hoe je toestemming hebt gekregen voor de verwerking van de persoonsgegevens.

Deze toestemming is pas geldig als het voldoet aan de volgende voorwaarden:

- De toestemming moet specifiek zijn
- De toestemming moet op informatie berusten
- De toestemming moet in vrijheid gegeven zijn
- De toestemming moet een actieve handeling zijn

Daarnaast moet je ook kunnen bewijzen dat je geldige toestemming hebt gekregen van het lid en moet het voor het lid net zo makkelijk zijn om de toestemming in te trekken als dat het was om de toestemming te geven.

Wat betekent dit voor jouw vereniging?
Wanneer een nieuw lid zich aanmeldt bij je vereniging, verstrekt het lid zijn persoonsgegevens. Hierbij dien je het nieuwe lid te informeren waarom jouw vereniging die specifieke persoonsgegevens nodig heeft. Het nieuwe lid moet deze redenen kunnen inzien voordat hij toestemming geeft. Nadat je de persoonsgegevens van het nieuwe lid hebt verkregen, mag je deze gegevens niet voor andere doeleinden gebruiken.

Het is dus belangrijk om goed in kaart te brengen waarom je persoonsgegevens opslaat en dat je deze redenen duidelijk communiceert met je leden. Ga dan ook na of alle gegevens die je opslaat daadwerkelijk noodzakelijk zijn voor de doeleinden die je opgeeft!

Vervolgens moet je bijhouden hoe en wanneer het lid zijn persoonsgegevens heeft verstrekt en hoe het lid toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.

Het lid moet ook net zo makkelijk zijn gegevens kunnen verwijderen als dat hij deze gegevens verstrekt heeft. Dat betekent dat als het lid bijvoorbeeld via een formulier op de website lid kan worden, het lid ook via een formulier op de website zijn gegevens moet kunnen (laten) verwijderen.

Datalek

Onder de AVG blijft de meldplicht van datalekken grotendeels gelijk aan die in de oude wetgeving. Er zijn echter wel strengere eisen aan de registratie van de datalekken die binnen jouw vereniging plaatsvinden. Je moet alle datalekken documenteren.

Wat is een datalek?
Een datalek is iedere inbreuk op de beveiliging waarbij persoonsgegevens verloren zijn gegaan, of ongeoorloofd zijn gewijzigd, verstrekt of ingezien. Bijvoorbeeld bij diefstal van een laptop met daarop een export van de ledenlijst, een oud bestuurslid dat onrechtmatig nog inlogt in de ledenadministratie in Congressus manager, het verzenden van gegevens naar een verkeerd e-mailadres of het verlies van een USB-stick met daarop gegevens van je vereniging.

Wat moet je doen bij een datalek?
Van ieder datalek moet je het volgende bijhouden:

- Een omschrijving van het lek;
- Wanneer vond het plaats;
- Wat is er met de gegevens gebeurd? Zijn ze door een onbevoegde ingezien, zijn ze verloren gegaan of onrechtmatig gewijzigd?;
- Van wie zijn de gegevens gelekt? Welke groep leden is het en om hoeveel leden gaat het;
- Om welke soorten gegevens het gaat;
- Wat zijn de (mogelijke) gevolgen van het lek? Denk aan identiteitsfraude, reputatieschade etc;
- Welke maatregelen zijn genomen naar aanleiding van het lek? Welke acties zijn ondernomen om de schade te voorkomen of zo veel mogelijk te beperken? En wat heb je er aan gedaan om dit voortaan te voorkomen?

Melden van een datalek
Een inbreuk in verband met persoonsgegevens moet je melden bij de toezichthouder (Autoriteit Persoonsgegevens), tenzij het lek geen risico oplevert op negatieve gevolgen als identiteitsfraude of reputatieschade. Indien je het lek moet melden aan de toezichthouder dan moet dit binnen 72 uur nadat de verwerkingsverantwoordelijke, de vereniging, kennis heeft genomen van het datalek dat gemeld moet worden.

In sommige gevallen moet je de leden waarvan de persoonsgegevens zijn gelekt op de hoogte stellen van het lek.

Procedure bij een datalek
Indien je je kennis hebt genomen van een datalek moet je een aantal stappen

ondernemen. Zorg ervoor dat je een procedure opstelt voor het adequaat anticiperen op, en afhandelen van een datalek. Op die manier heb je een leidraad op het moment dat een datalek plaatsvindt of heeft plaatsgevonden.

CHECKLIST

We hebben duidelijk beschreven met welk doel persoonsgegevens binnen onze organis
worden bewaard. Dit hebben we vastgelegd in een document.

We hebben vastgesteld en vastgelegd wie binnen de organisatie verantwoordelijk zijn vo
bescherming van persoonsgegevens (zoals bestuur, voorzitter, secretaris, Raad van To

---

We hebben een overzicht van alle persoonsgegevens die in één of meerdere bestanden
opgenomen zijn. Dit hebben we vastgelegd in een document.

Indien we bijzondere persoonsgegevens bewaren, dan is vastgesteld en vastgelegd wel
wettelijke uitzonderingsregel van toepassing is.

Bijzonder persoonsgegevens zijn: godsdienst of levensovertuiging, ras, politieke gezindh
gezondheid, medische informatie (medicijngebruik, allergieën), seksuele leven, lidmaats
van een vakvereniging of politieke partij, strafrechtelijke persoonsgegevens en
persoonsgegevens over onrechtmatig of hinderlijk gedrag in verband met een opgelegd
naar aanleiding van dat gedrag, genetische en biometrische kenmerken (vingerafdrukke
stem, handschrift, geometrie van de handomtrek en scans van netvlies, iris en gelaat).

Indien we bijzondere persoonsgegevens bewaren, dan vragen we bij elke activiteit waar
van belang is, opnieuw om toestemming om deze persoonsgegevens vast te mogen leg

---

Indien we bijzondere persoonsgegevens bewaren, dan vernietigen we na elke activiteit v
deze gegevens van belang zijn, deze persoonsgegevens.

We communiceren helder met betrokken personen over welke persoonsgegevens worde
bewaard. Het is duidelijk via welke kanalen zij worden geïnformeerd. Betrokken persone
kunnen zijn: leden, donateurs, deelnemers aan activiteiten, bezoekers van de website.

We vragen altijd toestemming aan betrokkenen om persoonsgegevens vast te leggen.

We vragen altijd toestemming aan betrokkenen om deze personen te mogen
fotograferen en de foto's te gebruiken voor communicatiedoeleinden (zoals publicatie op
website, sociale media, voor gebruik op folders of posters).

We hebben een protocol opgesteld voor personen die hun eigen persoonsgegevens in v
zien (inzagerecht). Dit hebben we vastgelegd in een document.

We hebben een protocol opgesteld voor personen die hun eigen persoonsgegevens will
wijzigen (correctierecht: rectificatie en aanvulling). Dit hebben we vastgelegd in een docu

---

We hebben een protocol opgesteld voor personen die hun eigen persoonsgegevens will
verwijderen (recht op vergetelheid). Dit hebben we vastgelegd in een document.

We hebben een protocol opgesteld voor personen die een beperking op de verwerking e
gebruik van hun eigen persoonsgegevens willen bewerkstelligen (recht op beperking van
verwerking). Dit hebben we vastgelegd in een document.

We hebben een protocol opgesteld voor personen die bezwaar maken tegen de verwerk
hun eigen persoonsgegevens (recht op bezwaar). Dit hebben we vastgelegd in een docu

We hebben een protocol opgesteld voor personen die hun eigen persoonsgegevens will meenemen naar een andere organisatie (recht op dataportabiliteit). Dit hebben we vastg in een document.

Indien onze organisatie leden heeft, dan worden gegevens van oud-leden uiterlijk twee j het lidmaatschap uit de actieve ledenadministratie verwijderd (tenzij een oud-lid al eerde aangegeven zijn persoonsgegevens verwijderd dienen te worden uit de actieve ledenadministratie).

We hebben een overzicht van de plaatsen waar bestanden met persoonsgegeven worde bewaard (in fysieke mappen, computer, cloud, …)

Indien we kopieën of back-ups hebben gemaakt met bestanden met persoonsgegevens bekend waar en hoe deze worden bewaard.

We hebben maatregelen genomen om te voorkomen dat onbevoegden persoonsgegeve kunnen inzien. Wie binnen de organisatie toegangsrechten heeft om persoonsgegevens zien en te wijzigen, hebben we vastgelegd in een document.

We hebben een functionaris voor de gegevensbescherming aangesteld binnen onze organisatie.

We hebben met alle externe partijen die onze persoonsgegevens verwerken, een verwerkersovereenkomst afgesloten. Dit kunnen externe partijen zijn als een koepelorga (sportbond, landelijke bureau van een lokale organisatie), verzender nieuwsbrief, websit

hoster.

In de verwerkersovereenkomsten met externe partijen is opgenomen hoe lang de persoonsgegevens bewaard blijven en wanneer deze na gebruik vernietigd worden.

We hebben een procedure opgesteld voor het melden van datalekken. Dit is vastgelegd document.

We hebben een procedure opgesteld over de communicatie met betrokkenen in het gev een datalek. Dit is vastgelegd in een document.

Onze website is afdoende beveiligd tegen hacken. Dit is mogelijk door middel van een beveiligingscertificaat.

De ICT systemen (zoals pc, laptop, tablet) waar we bestanden met persoonsgegevens b of waarmee we toegang kunnen krijgen tot deze bestanden, zijn afdoende beveiligd tege hacken, virussen, malware.

We hebben een privacyverklaring geplaatst op onze website waarin beschreven staat da persoonsgegevens verzameld worden (indien van toepassing) en wat er met de data ge wordt.

We hebben onze vrijwilligers geïnformeerd en/of opgeleid welke procedures er binnen d organisatie zijn voor het omgaan met persoonsgegevens.

Indien er sprake is van cameratoezicht, melden we dit aan bezoekers van onze accommodatie/terrein/pand.

Indien er sprake is van cameratoezicht, dan verwijderen we de beelden na vier weken.

Indien er sprake is van cameratoezicht, dan hebben we een protocol opgesteld om betro inzage te geven in de beelden (recht op inzage). Dit is vastgelegd in een document.

Disclaimer: deze checklist is met de grootste zorg samengesteld. Ik ben geen jurist en aanvaardt geen enkele aansprakelijkheid als er onvolkomenheden in de checklist staan. Mocht je inhoudelijke (juridische) vragen hebben over jouw eigen situatie, leg je vraag dan voor aan een jurist.