ShantyNederland nieuwsbrief

64

"Van zingen wordt een mens blij"

"Van zingen wordt een mens blij" is een bekende uitspraak. Uiteraard ben ik als lid van mijn koor het hier hartgrondig mee eens. Als penningmeester van ShantyNederland gebeurt het echter nog wel eens dat mijn zingen een klaagzang wordt. Daarom vraag ik graag nog een keer uw aandacht voor een aantal zaken die nog wel eens fout gaan.
Zo is het nog wel eens lastig betalingen van de contributienota terug te vinden door het ontbreken van het factuurnummer. Dit is zeker het geval wanneer de contributie wordt betaald vanaf een privébankrekening. Zonder de naam van het koor erbij wordt het nog wel eens de bekende speld in de hooiberg.
Ook komt het voor dat er op een herinnering ook geen reactie komt. Dan is het wel duidelijk dat er inmiddels een ander e-mailadres gebruikt wordt en begin ik een speurtocht via website en telefoon naar het nieuwe adres. Bestuurswisseling in het secretariaat krijgen wij daarom graag van u door.
Verder complimenten aan de koren voor het betaalgedrag. Wij hebben nagenoeg geen moeilijke betalers en dat is fijn in verband met onze verplichtingen naar derden.
Voor zover een tevreden penningmeester Frits.

Wel is mij meerdere malen gevraagd hoe de "machtstructuren" binnen een vereniging precies liggen.

Binnen de vereniging zijn er twee machtscentra: de Algemene Ledenvergadering en het bestuur. Maar wie heeft het nu voor het zeggen?

Het bestuur is het deskundig en continu leidinggevend orgaan: het bestuurt de vereniging. De Algemene Ledenvergadering (ALV) is het orgaan dat bestaat uit de leden, die de hoogste zeggenschap hebben. Maar de Algemene Ledenvergadering mag niet op de stoel van het bestuur gaan zitten. Het bestuur heeft een geheel eigen verantwoordelijkheid met daarbij behorende bevoegdheden. De ALV is niet de baas van het bestuur en kan geen opdrachten geven hoe het moet besturen. De ALV kan hooguit een bestuurder of het bestuur naar huis sturen. Met dat in het achterhoofd doet een bestuur er dus goed aan te handelen in de geest van de meerderheid van de leden.
Waarvan acte!!

vervolg blz 1.

Algemene Verordening Gegevensbescherming

Op 25 mei 2018 treedt bovengenoemde verordening in werking.
Van koornetwerk nederland hebben wij informatie gekregen betreffende deze verordening, welke van toepassing is voor alle organisaties (lees verenigingen) die gegevens van personen in een bestand bewaren.

In deze nieuwsbrief hebben wij een vragenbrief en stappenplan, opgesteld door koornetwerk nederland, bijgevoegd. U kunt zich hiermede op de hoogte stellen van deze verordening. In een later stadium zal er zeker nog meer hierover in de media verschijnen.

Frits van Kouwen

Privacybeleid Algemene Verordening Gegevensbescherming

Vragenlijst
Privacybeleid Algemene Verordening Gegevens bescherming

De nieuwe Algemene Verordening Gegevensbescherming vraagt van organisaties een aantal antwoorden die in het privacybeleid moeten worden opgenomen. Onderstaande vragen kunnen je helpen het privacybeleid vorm te geven.

1. Met welk doel worden persoonsgegevens in een bestand bewaard?

2. Wie binnen de organisatie zijn verantwoordelijk voor de bescherming van persoonsgegevens (bestuur, directie,...)

3. Welke persoonsgegevens worden in het bestand opgenomen, is daar een overzicht van?

4. Worden er bijzondere persoonsgegevens bewaard (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)? En welke wettelijke uitzonderingsregel is van toepassing?

5. Hoe worden de personen geïnformeerd over welke persoonsgegevens worden bewaard?

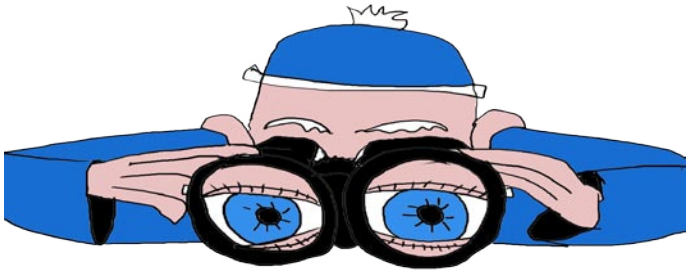
6. Wat is er geregeld voor personen om hun eigen persoonsgegevens in te zien?

7. Hoe worden de persoonsgegevens bewaard (in fysieke mappen, computer, cloud, ...)?

8. Zijn er kopieën of wordt er een back-up van het gegevensbestand gemaakt en hoe wordt die bewaard?

9. Welke maatregelen heeft de organisaties genomen om te voorkomen dat andere onbedoeld persoonsgegevens kunnen inzien?

10. Wie binnen de organisatie hebben toegang tot de bestanden met de persoonsgegevens?



TAAIE KOST, maar wel lezen!!!!

E: info@koornetwerk.nl
I: www.koornetwerk.nl

1 januari 2018

Stappenplan Algemene Verordening
Gegevensbescherming (AVG)

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 op geborgen zonder dat vreemden daar bij kunnen. Met onderstaande zes 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 verstrekten 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 (zie 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. (zie privacy beleid)

Stap 4: Stel 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 ver werken in opdracht van en verantwoordelijke;
- FG'S moeten passende technische en organisatorische beveiligingsmaatregelen nemen die een pas send 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 ver werken (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 onmiddelijk op de hoogte stellen van een datalek. De termijn voor 'onverwijld' in de Nederlandse wetgeving wordt in de Wet Meldplicht datalekken door de Autoriteit Persoonsgegevens (AP) vastgesteld op 72 uur na ontdekking van het incident;

- FG'S zijn verplicht medewerking te verlenen aan verzoeken van de AP in het kader van de uitoefening van zijn taken;
- In bepaalde gevallen moet de FG een Privacy Impact Assessment uitvoeren. In ieder geval bij profiling, verwerken van bijzondere persoonskenmerken en opslaan van camerabeelden met personen;

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 camera toezicht) Voor de meeste vrijwilligersor ganisaties is een formele PIA niet nodig. Vooral niet omdat alleen contactgegevens verzameld worden en geen persoonskenmerken.

Stap 6: Vrijwilligers informeren of opleiding bieden over het omgaan met persoonsgegevens.
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 hiervoor vooraf procedures af te spreken en vast te leggen.
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.

AGENDA

Februari

2en3..Putten - Workshop ShantyNederland
4...Enkhuizen - Prelude Deunen en Deinen
4...Vlaardingen - 36e ShantyCafé
16 t/m 18..Schiermonnikoog - Zangweekend
17..Hardinxveld Giessendam - Ierse avond
18..Rotterdam - 82e ShantyCafé
21+28..Podium Vlieland - Drijfhout, met een korreltje zout
23 t/m 25..Enkhuizen - Winter Shantyfestival Deunen en Deinen
25..Enkhuizen - Workshop met Kimber's men
24..Winsum Fr. - 10e Sjongersdei

Maart

4...Vlaardingen - 37e ShantyCafé
17..Roswinkel - Theaterboerderij De Noorderbak
18..Rotterdam - 83e ShantyCafé
21+28..Podium Vlieland - Drijfhout, met een korreltje zout
31..Kampen - Zeemanskorenfestival

WIJZIGING DOORGEVEN

Hoe geef ik door aan ShantyNederland dat de contactpersoon wijzigt?
Het komt bij elk koor regelmatig voor dat de functies binnen het Bestuur wijzigen. Om dat tijdig door te geven aan Shanty Nederland stuurt één van de bestuursleden – meestal de secretaris – een mail aan Shanty Nederland met de mededeling dat er een wisseling binnen het bestuur heeft plaatsgevonden en dat bijvoorbeeld de penningmeester wijzigt of er is een nieuw mailadres dat voortaan gebruikt moet worden. Soms ook een nieuw mailadres voor de secretaris en een ander mailadres voor de penningmeester waar dan de nota naar toe moet.
De indiener krijgt in dat geval het verzoek van de secretaris van Shanty Nederland om voor wijzigingen het formulier op de website van Shanty Nederland te gebruiken voor het doorgeven van wijzigingen. Niet alleen als het mailadres wijzigt maar ook als de contactpersoon wijzigt.
De contactpersoon krijgt namelijk alle mail en post die Shanty Nederland aan haar leden stuurt.
Wij kunnen echter maar 1 mailadres opnemen; het zou ontzettend veel werk met zich meebrengen – en gemakkelijk fouten in de hand werken – als we van alle 368 koren die lid zijn moeten bijhouden wie wanneer welke informatie we moeten sturen.

Hieronder staat een voorbeeld Mutatieformulier

Koor / Groep:	Shantykoor De Zingende Zeiltjes
Keuzelijst: wijziging/aanvulling	wijziging
Naam:	Froukje Fokkeschoot
Adres:	Stuurboorwal 333
Postcode - Plaats:	2099 ZZ Havenplaats
Telefoon nr.:	06 - 22211999
Email:	info@zingendezeiltjes.nl
HerhaIen email:	info@zingendezeiltjes.nl
Opmerkingen	Nieuwe secretaris i.p.v. Hendrik van Ham

Vragenlijst
Privacybeleid Algemene Verordening Gegevensbescherming

De nieuwe Algemene Verordening Gegevensbescherming vraagt van organisaties een aantal antwoorden die in het privacybeleid moeten worden opgenomen. Onderstaande vragen kunnen je helpen het privacybeleid vorm te geven.

1. Met welk doel worden persoonsgegevens in een bestand bewaard?

2. Wie binnen de organisatie zijn verantwoordelijk voor de bescherming van persoonsgegevens (bestuur, directie,...)

3. Welke persoonsgegevens worden in het bestand opgenomen, is daar een overzicht van?

4. Worden er bijzondere persoonsgegevens bewaard (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)? En welke wettelijke uitzonderingsregel is van toepassing?

5. Hoe worden de personen geïnformeerd over welke persoonsgegevens worden bewaard?

6. Wat is er geregeld voor personen om hun eigen persoonsgegevens in te zien?

7. Hoe worden de persoonsgegevens bewaard (in fysieke mappen, computer, cloud, ...)?

8. Zijn er kopieën of wordt er een back-up van het gegevensbestand gemaakt en hoe wordt die bewaard?

9. Welke maatregelen heeft de organisaties genomen om te voorkomen dat andere onbedoeld persoonsge gevens kunnen inzien?

10. Wie binnen de organisatie hebben toegang tot de bestanden met de persoonsgegevens?

11. Is er een functionaris voor de gegevensbescherming in de organisatie?

12. Zijn er afspraken gemaakt met externe partijen die de persoonsgegevens verwerken, is er een verwerkers overeenkomst?

13. Worden er overeenkomsten afgesloten met derden die de persoonsgegevens gebruiken en staat daar in dat de bestanden na gebruik vernietigd worden?

14. Heeft een de organisatie een procedure opgesteld voor het melden van datalekken, en staat die op papier?

Digitale nieuwsbrief van ShantyNederland
met bijdragen van koorleden en bestuursleden.
Opmaak en illustraties: Jan Huttinga