GDPR voor verenigingen stap voor stap…

In het kort: wat is 'GDPR'?

GDPR is de afkorting van "General Data Protection Regulation", in het Nederlands spreken we over AVG of "Algemene Verordening Gegevensbescherming".

Deze regeling heeft als doel om de privacy van burgers te beschermen en wil verhinderen dat onze persoonsgegevens zomaar overal te grabbel gegooid worden. GDPR wil onze gegevens beschermen door verplichtingen op te leggen aan organisaties die persoonsgegevens bezitten of verwerken.

De regels opgelegd door GDPR traden reeds in werking op 25 mei 2018. Dit wil zeggen dat in principe alle verenigingen reeds in regel moeten zijn. Is dit niet het geval, tracht dit dan zo snel mogelijk in orde te brengen!

Aan de hand van onderstaande informatie willen we jullie op een overzichtelijke manier helpen om door de bomen het bos te zien. We hopen jullie te kunnen ondersteunen bij de opmaak van jullie GDPR-verhaal.

Basisprincipes!

De regels en verplichtingen rond GDPR zijn opgebouwd rond een aantal basisprincipes. Als vereniging moet men zich drie vragen stellen die leiden tot de antwoorden op de basisprincipes.

Vraag 1 ~ Verwerkt uw vereniging persoonsgegevens ?

Persoonsgegevens = alle informatie die hoort bij een bepaalde natuurlijke persoon en deze persoon identificeert (naam, voornaam, adres, bloedgroep, telefoonnummer, gsm-nummer,…).

Verwerken = het verzamelen, opslaan, gebruiken, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, gebruiken, verstrekken, verspreiden, wissen of vernietigen,… van persoonsgegevens al dan niet uitgevoerd via geautomatiseerde procedés.

Vraag 2 ~ Mag uw vereniging persoonsgegevens verwerken ?

Persoonsgegevens kunnen ondergebracht worden onder twee categorieën, enerzijds hebben we een aantal situaties die vallen onder noodzakelijkheid (in dat geval is er niet veel actie vereist), anderzijds zullen bepaalde situaties vallen onder het verkrijgen van een toestemming (in dat geval is er wat meer werk aan de winkel). Indien men noch onder de eerste, noch onder de tweede categorie valt, dan is het verwerken van persoonsgegevens niet toegelaten!

CATEGORIE 1 : De situaties van noodzakelijkheid…

1. **Noodzakelijk voor het uitvoeren van een overeenkomst**

   Wanneer men een overeenkomst of contract afsluit met iemand, dan is het niet meer dan logisch dat een aantal persoonsgegevens verwerkt worden. Om een overeenkomst af te sluiten, moet je weten wie de andere persoon is. Let wel op: de verwerking moet noodzakelijk zijn voor de uitvoering van de overeenkomst!

   Om in deze categorie te vallen moet aan volgende voorwaarden voldaan worden:

- er is een contract nodig;
- er is geen expliciete goedkeuring nodig voor het verwerken van de persoonsgegevens van de persoon die het contract afsluit;
- de vereniging moet over een privacyverklaring beschikken waarin de tegenpartij wordt geïnformeerd.

2. **Noodzakelijkheid om te voldoen aan de wettelijke verplichtingen**

   Het kan zijn dat de wet of een andere reglementering verplicht om een aantal persoonsgegevens te verwerken.

   Om in deze categorie te vallen moeten volgende voorwaarden voldaan worden:

   - Er moet een wettelijke of reglementaire verplichting bestaan tot het bijhouden van de gegevens;
   - Hier wordt geen toestemming van de persoon waarvan men de gegevens verwerkt, vereist;
   - de vereniging moet over een privacyverklaring beschikken.

3. **Noodzakelijkheid voor de behartiging van gerechtvaardigde belangen**

   Om onder deze situatie te vallen, moet uw vereniging dus enerzijds een belang hebben (er moet een noodzaak zijn voor de vereniging) en anderzijds moet dat belang gerechtvaardigd (verwerking mag niet opdringerig of ongepast zijn) zijn.

   Voorbeelden van deze noodzakelijkheid zijn: direct marketing, doelgroepen contacteren, gegevens vrijwilligers/sponsors/… verzamelen,…

CATEGORIE 2 : het verkrijgen van expliciete toestemming…

Wanneer men geen grond of situatie vindt in categorie 1, kan men toch nog persoonsgegevens verwerken indien men de expliciete toestemming bekomt van de betrokkene. Bij deze categorie volstaat een beschrijving in de privacyverklaring niet en moet men expliciet om toestemming vragen.

CATEGORIE 3 : noch noodzakelijk, noch expliciete toestemming…

Wanneer men zich niet kan baseren op situaties onder noodzakelijkheid én er geen expliciete toestemming is van de betrokkenen mogen er **GEEN** persoonsgegevens worden verwerkt.

Vraag 3 ~ Welke aandachtspunten/principes moet uw vereniging in acht nemen als persoonsgegevens worden verwerkt ?

Enkele beginselen en principes die in acht moeten genomen worden:

- persoonsgegevens kunnen enkel voor een welbepaald doel worden verwerkt;
- het verwerken van persoonsgegevens moet beperkt gebeuren, dat wil zeggen dat men niet teveel gegevens mag opvragen en/of bijhouden;
- de persoonsgegevens moeten steeds juist en actueel zijn;
- de persoonsgegevens mogen worden verwerkt zolang dat nodig is;
- de organisatie moet voorzien in een passende beveiliging om de persoonsgegevens te beveiligen en te beschermen;
- men mag enkel persoonsgegevens verwerken wanneer dit op een rechtmatige en transparante manier gebeurt.

Het GDPR-stappenplan voor verenigingen !!!

Documenten opmaken	**1** Inventaris	**2** Dataregister	**3** Privacyverklaring		
Beveiligen + aanpassen	**4** Bewust maken	**5** Beveiligen	**6** Toestemming check	**7** Website check	**8** Contracten check
Procedures voorzien	**9** Datalekken	**10** Rechten Burgers			
~~+ Extra~~	~~Personeel~~	~~Functionaris~~	~~Interne audit~~	~~Internationaal~~	

Stap 1: Inventaris

In deze stap is het de bedoeling om in kaart te brengen welke persoonsgegevens uw vereniging allemaal bijhoudt en hoe dat gebeurt.

1. Opsommen van wie er allemaal persoonsgegevens worden bijgehouden in uw vereniging en wat daarvan de rechtsgrond is.
2. Welke persoonsgegevens worden bijgehouden en hoe worden ze bewaard/beveiligd?
    a. Welke persoonsgegevens worden bewaard?
    b. Waar worden de persoonsgegevens bewaard?
    c. Hoe lang worden de persoonsgegevens bewaard?
    d. Wie heeft toegang tot de persoonsgegevens?
    e. Worden de persoonsgegevens beschermd of beveiligd?
    f. Waarvoor worden de persoonsgegevens juist gebruikt?
    g. Aan wie worden persoonsgegevens (eventueel) doorgegeven?

Geef deze informatie weer in tabellen om de overzichtelijkheid te garanderen. U kan een blanco document terugvinden in dit pakket. In het grijs kan u voorbeelden terug vinden, neem deze niet letterlijk over.

Stap 2: Stel een dataregister op en houd dat up-to-date

In een dataregister maakt u een overzicht van de persoonsgegevens die uw vereniging verwerkt en bepaalt u ook duidelijk waar ze vandaan komen, met wie ze gedeeld worden en op welke grond ze zijn verzameld.

Het is een verplichting voor het bestuur van de vereniging om het dataregister up-to-date te houden!

De gegevens die u opnam in de inventaris zijn de basis voor het opstellen van het dataregister. Om de opmaak van het dataregister op een gemakkelijke en gestructureerde manier aan te pakken, kan u de tabel gebruiken die u in dit pakket terugvindt. U vult deze opnieuw in voor elke groep van personen waarvan u persoonsgegevens verwerkt. Wanneer u de verschillende tabellen bundelt heeft u een eenvoudig, maar correct dataregister. In dit pakket kan u in grijze tekst een voorbeeld terugvinden, neem dit niet letterlijk over.

Stap 3: Stel een privacyverklaring op en verwijs ernaar

De privacyverklaring is een document waarin een vereniging de betrokkenen waarvan de persoonsgegevens worden verwerkt, proactief informeert over een aantal zaken (het gebruik van de persoonsgegevens, de rechten van de betrokkenen,…). De privacyverklaring moet heel duidelijk zijn, in eenvoudige taal opgesteld worden, beknopt en transparant zijn. De privacyverklaring moet dan ook vlot toegankelijk zijn. Dit kan door deze te publiceren op de website, in het huishoudelijk reglement,…

De privacyverklaring moet een aantal gegevens bevatten:

- identiteit verwerkingsverantwoordelijke, dat is uw vereniging;
- de soorten persoonsgegevens die worden verwerkt;
- doeleinden waarvoor de gegevens worden verwerkt;
- de wijze waarop uw vereniging de gegevens zal aanwenden;
- de wettelijke grondslag voor gegevensverwerking;
- verstrekking van de gegevens aan verwerkers en derden;
- de termijnen gedurende dewelke uw vereniging de informatie bijhoudt;
- of uw vereniging de gegevens uitwisselt buiten de Europese Unie;
- de mogelijkheid voor de betrokkene om een klacht in te dienen bij de Gegevensbeschermingsautoriteit indien hij/zij meent dat zijn/haar persoonsgegevens foutief worden verwerkt;
- de rechten van de betrokkenen personen
- de technische en organisatorische maatregelen die uw vereniging zal nemen om in orde te zijn;
- een aantal bepalingen omtrent het portretrecht (dat is belangrijk wanneer beelden worden genomen op activiteiten).

U kan een model voor het opstellen van een privacyverklaring terugvinden in dit pakket. Pas dit zeker nog aan aan uw vereniging en vul verder aan.

Stap 4: Zorg ervoor dat iedereen binnen uw vereniging bewust wordt van GDPR

Iedereen die in uw organisatie werkt met persoonsgegevens, moet zich er heel bewust van zijn dat hij of zij hier omzichtig mee moet omgaan. Daarom is het belangrijk om deze personen goed te informeren over:

- het belang van privacy;
- de voorwaarde waaronder persoonsgegevens bewaard en verwerkt kunnen worden;
- de stappen die uw organisatie onderneemt om zich in regel te stellen.

Het is belangrijk om het onderwerp ‘GDPR’ te agenderen op de bestuursvergadering, bijeenkomst van het bestuursorgaan en de Algemene Vergadering. Neem dit agendapunt ook duidelijk op in het verslag, zo kan uw organisatie aantonen dat de nodige acties werden ondernomen.

Stap 5: Zorg voor een goede beveiliging

Privacygevoelige gegevens vragen de nodige bescherming en beveiliging. Het is dan ook niet meer dan logisch dat u als organisatie hiervoor de nodige maatregelen neemt. Deze maatregelen kunnen zowel organisatorisch als technisch zijn.

> Organisatorische maatregelen: afspreken wie over bepaalde persoonsgegevens kan beschikken.
> Technische maatregelen: een afgesloten kast in het verenigingslokaal, beveiligen van computer, wachtwoordengebruik,…

Stap 6: Check toestemmingen

Het is perfect mogelijk om persoonsgegevens te verwerken als er een rechtmatige grond toe bestaat. Ofwel bestaat de grond uit een noodzakelijkheid, ofwel heeft u de expliciete toestemming van iemand nodig. Indien u persoonsgegevens via expliciete toestemming heeft verworven, is het nodig om na te gaan of die toestemming wel correct werd gegeven.

Opgelet, indien het gaat om een minderjarige die een 'contract' of 'overeenkomst' afsluit, dan zullen zij dat enkel kunnen doen met instemming van hun ouders of voogd.

Stap 7: Websitecheck

De website van uw organisatie moet ook aangepast worden aan de GDPR-wetgeving.

1. Zorg ervoor dat op de website op elke pagina een link staat naar de privacyverklaring. De privacyverklaring zelf zet u dus ook volledig online.
2. Wanneer de website gebruik maakt van cookies dan moet de toestemming van de bezoekers van die website hiervoor gevraagd worden. Dit gebeurd door een eenvoudige pop-up met de vraag om akkoord te gaan.
3. Wanneer persoonsgegevens via de website worden verzonden heeft men een SSL-certificaat voor de website nodig. Dit zorgt voor een beveiligde verbinding.

Stap 8: Check contracten

Het is belangrijk om te checken bij welke contracten die de organisatie afsloot het verwerken van persoonsgegevens aan bod komt. Indien dat het geval is, dan moet een verwerkingsovereenkomst afgesloten worden. Hierin moet duidelijk worden uitgelegd wie welke verantwoordelijkheid draagt en hoe derde-partijen met persoonsgegevens moeten omspringen.

Stap 9: Procedures voorzien

Datalekken zijn situaties waarbij de persoonsgegevens op één of andere manier openbaar worden of in andere handen terechtkomen. Het is verplicht om bij een datalek zonder onredelijke vertraging binnen 72 uur na kennisname te melden bij de toezichthoudende autoriteit. Daarnaast moet dit onmiddellijk gemeld worden aan de betrokkene. Enkel wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de betrokken persoon.

Duid binnen het bestuursorgaan een verantwoordelijke aan die de nodige en correcte actie onderneemt wanneer zo'n datalek zich voordoet.

U kan een aangifte online doen via de website van de Gegevensbeschermingsautoriteit (GBA): https://www.gegevensbeschermingsautoriteit.be/meldformulier-voor-gegevenslekken.

Stap 10: Rechten van de burgers

Doordat persoonsgegevens als het ware aan uw persoon 'kleven', bezit u bepaalde rechten. Als vereniging moet u zich er bewust van zijn dat deze rechten van burgers gerespecteerd moeten worden.

- Recht op informatie
- Recht op inzage en kopie
- Recht op rectificatie (wijzigen/aanpassen)
- Recht op gegevenswissing – vergetelheid
- Recht op verzet
- Recht op bezwaar
- Recht op overdraagbaarheid van gegevens.

Indien de vereniging een verzoek tot het uitoefenen van rechten krijgt moet de vereniging gevolg geven aan het verzoek binnen één maand. Wanneer er geen gevolg wordt gegeven aan het verzoek moet dit gemotiveerd worden aan de betrokkene binnen eveneens één maand na ontvangst van het verzoek.