In orde met GDPR

De GDPR (General Data Protection Regulation) of AVG (Algemene Verordening Gegevensbescherming) is een geheel van Europese regels om de burger te beschermen rond gebruik van persoonsgegevens. Ze is van toepassing sinds 25 mei 2018.

Elke organisatie, ook vzw's en feitelijke verenigingen die persoonsgegevens gebruiken, opslaan of verwerken, vallen onder de regelgeving en moeten zich in orde stellen.

De EU ziet 'persoonsgegevens' immers erg breed. Ook IP-adressen, cookies en Twitter-handles worden bijvoorbeeld gezien als persoonsgegevens.

Via het 7 stappenplan kan u zich in orde stellen met GDPR. Er zijn templates voorzien om de stappen te ondersteunen.

In het kort – Je moet zeker hebben:

- Een gegevensregister waarin staat wat de rechtsgrond is om gegevens bij te houden. Welke gegevens je bijhoudt, wat je ermee doet, waar ze bewaard worden, hoe ze beveiligd zijn en hoe je ze bewaart…
- Een privacyverklaring voor de federatie en voor je club
- Hoe kunnen mensen hun gegevens opvragen, verbeteren of laten verwijderen?
- Hoe beveilig je de gegevens en hoe volg je een data lek op?
- Verzeker je van de garantie GDPR van alle derden waarmee je gegevens deelt.
- Zorg ervoor dat alle derden waarmee je gegevens van leden deelt ook conform de nieuwe regels rond GDPR werken. (Schriftelijk bewijs)

Toestemming

Er is een doelbinding of legaliteitsbinding voor de gegevens die RV gebruikt. Het bezorgen van informatie en uitnodigingen over werking en activiteiten is een onderdeel van het lidmaatschap.

Nieuwsbrieven: digitale nieuwsbrieven behoren tot de legaliteitsbinding. Als je echter nieuwsbrieven wil versturen aan sympathisanten, oud-leden of occasionele deelnemers dan moet je hiervoor een uitdrukkelijke toestemming hebben. RV zal toestemming vragen aan niet-leden via een "your Mail List Delivery" platvorm. (dat nadrukkelijke toestemming vraagt alvorens je de nieuwsbrief kan lezen en deze toestemming registreert).

Foto's en beeldmateriaal: zijn verwerking van persoonsgegevens. Je moet toestemming vragen van de persoon in kwestie voor gerichte foto's en beelden. Om het beeldmateriaal te gebruiken heb je voor gerichte beelden ook toestemming nodig. (Mondeling is gewoonlijk voldoende, maar schriftelijk is bewijsbaar) Ook dit materiaal volgt alle regels conform de GDPR.

Je kan de toestemming van niet-leden voor nieuwsbrieven en het gebruik van beeldmateriaal vragen op het inschrijvingsformulier voor organisaties.

GDPR en de rugbyclubs

Rugby Vlaanderen en haar clubs delen dezelfde ledendatabase. De clubs houden de getekende inschrijvingsformulieren van hun leden bij waarop ook een vak GDPR toestemming staat. RV laat aan haar clubs weten dat ze beantwoordt aan de GDPR wetgeving (via e-mail aan het clubbestuur). De secretarissen van de clubs brengen per seizoen alle leden van hun club in bij deze database. Op het einde van elk seizoen wordt deze ledendatabase terug op nul gezet. (Nadat een lidmaatschap gestopt is, worden sommige leden gegevens nog 3 jaar bijgehouden andere tot maximum 5 jaar. Daarna worden ze verwijderd. De gescande medische fiches worden verwijderd bij einddatum attest – maximum 2 jaar). Een club kan alleen haar eigen leden opvragen via een beveiligde entry.

Om het voor onze clubs eenvoudiger te maken hebben we op de website van Rugby Vlaanderen een speciale GDPR pagina aangemaakt. Daar vindt je alle info die je nodig hebt en een aantal hulpmiddelen:

- Een template voor je privacy verklaring
- Een word document om een inventaris te maken
- Een word document om je inventaris te toetsen aan de EU GDPR wetgeving
- Een document om eventuele datalekken te melden

In orde met GDPR in 7 stappen

1) Creëer bewustzijn rond GDPR bij alle betrokkenen

Iedereen bij Rugby Vlaanderen en alle medewerkers binnen een club die in contact komen met persoonsgegevens, moeten op de hoogte zijn van de wetgeving rond GDPR en de noodzakelijke wijzigingen ondersteunen rond gegevensbescherming en privacy.

Actie: RV plant een workshop GDPR voor medewerkers RV en clubs.

We zijn allemaal gevoelig aan privacy-issues en GDPR zal dat nog meer in de kijker zetten. Communiceer daarom duidelijk over je privacy beleid.

2) Maak een inventaris en leg een dataregister aan

Actie: **Maak een inventaris op** van al je huidige gegevensbestanden met een overzicht van de persoonsgegevens.

Actie: Toets of je data GDPR conform is en plan de aanpassingen.

Als onderdeel van de documentatieplicht moet elk bedrijf en elke vereniging een dataregister hebben. Als er ooit een data lek is, zal je dat register moeten voorleggen om te bewijzen dat je wel degelijk de regels gevolgd hebt.

Actie: Leg een dataregister aan met waarom en de wijze waarop je de gegevens aanwendt. Verklaar ook waar ze vandaan komen, met wie ze gedeeld worden en wie de verwerkers zijn. In het dataregister moet je verder meedelen:

- Waarom, ga je Welke gegevens Hoe en Waar verwerken?
- Hoe, Waar en Hoelang ga je ze bijhouden?
- Hoe worden de gegevens beveiligd
- Worden ze uitgewisseld, intern en/of extern binnen, buiten de Europese Unie?

3) Bepaal noodzaak en wettelijkheid en communiceer in klare taal

Legaliteitsvereiste. Persoonlijke data verwerken mag enkel als het noodzakelijk is voor de uitvoering van de diensten, als er een wettelijke verplichting bestaat of als je hiervoor de toestemming hebt gekregen. Dat noemt men **doelbinding of dataminimalisatie**.

Proportionaliteitstoets. Je zal zelf kritisch moeten onderzoeken **waarom je data hebt** en of je die wel echt nodig hebt. Persoonlijke data mag je ook niet onbeperkt bewaren. Gegevens van prospects of cv's van sollicitanten zullen bijvoorbeeld geen jaren in je bezit mogen blijven.

Actie: Stel een privacyverklaring op en zet ze op je website. (verwijs in je documenten naar je privacyverklaring)

Transparantie. Alle betrokkenen moeten duidelijk geïnformeerd worden

Actie: Zorg er voor dat je documenten conform zijn aan de nieuwe GDPR wetgeving en leg uit in klare taal. (privacyverklaring, inschrijvingsformulier, doktersattest, contracten en ongevalsaangifte…)

'Privacy By Design' is de norm die gehanteerd moet worden in het kader van de GDPR. Dat betekent dat voor de ontwikkeling van (nieuwe) producten en diensten zoals websites, aandacht moet besteed worden aan privacy-verhogende maatregelen. Van zodra je data anonimiseert, is het niet langer persoonlijke data en is dus de privacy niet van toepassing.

4) Vraag en controleer de toestemming

De wijze waarop je toestemming vraagt om iemands persoonsgegevens te verwerken, moet volgens de GDPR **vrij, specifiek, geïnformeerd en ondubbelzinnig** zijn.

Voorbeeld: Het verplicht moeten doorgeven van je locatiegegevens als je je zaklamp van je smartphone wil gebruiken, is geen vrije toestemming. Er is geen reden waarom je smartphone moet weten waar je bent om je zaklamp te kunnen gebruiken.

De toestemming moet ook blijken uit een **actief handelen**. Er kan bijvoorbeeld geen sprake zijn van een geldige toestemming als die afgeleid wordt uit een vooraf aangevinkt keuzevakje.

Actie: Naast het vragen en verkrijgen van de toestemming is de registratie ervan ook van belang. De toestemming moet immers controleerbaar zijn. Je moet dus achteraf kunnen bewijzen dat je, voor elk persoonlijk gegeven dat je verwerkt, op een correcte manier toestemming kreeg om het te verzamelen.

Voor de verwerking van persoonsgegevens van **minderjarigen** heb je een specifieke toestemming van de ouder of voogd nodig.

5) Waar hebben betrokkenen recht op?

De betrokkenen moeten over hun rechten rond persoonsgegevens en privacy geïnformeerd worden:

- Recht op inzage kopie, verbetering, beperking én verwijdering van gegevens
- Recht op bezwaar tegen direct marketingpraktijken, geautomatiseerde besluitvorming en profilering;
- Recht op overdraagbaarheid van de gegevens. Iedereen moet zijn persoonsgegevens in een gangbare elektronische vorm kunnen opvragen.
- Recht op klacht bij de privacy commissie

Actie: Denk na over de procedures die je gaat volgen om aan dit soort vragen van particulieren tegemoet te kunnen komen.

6) Maak een data rampen plan

Volgens de GDPR moet je op voorhand bepalen hoe je het zal oplossen als het ooit fout loopt met je data.

Actie: Bouw dus adequate procedures uit die het mogelijk maken datalekken zo snel mogelijk op te sporen, te onderzoeken en sinds 25 mei 2018 ben je verplicht een **data lek te melden binnen de 72 uur aan de overheid** (bv. aan de Privacy commissie). In sommige gevallen zal de betrokkene zelf (wiens data gelekt is) ook ingelicht moet worden.

7) Stel een verantwoordelijke GDPR aan

De federatie of haar clubs moeten geen 'Data Protection Officer' aanstellen.

Actie: Stel een GDPR verantwoordelijke aan die een stappenplan uitvoert en opvolgt.

Als je data verwerkt of doorgeeft buiten de EU (bv. gegevens die op een server in de US staan), zal je moeten nagaan of dat land over eenzelfde soort van privacywetgeving beschikt als in de EU het geval is. Slechts een beperkt aantal landen voldoet hieraan. Vaak moeten een aantal garanties met de internationale partijen onder meer contractueel worden afgedwongen.

Actie: Vraag garantie GDPR aan derden waarmee je gegevens deelt. Controleer je datastromen dus en zorg dat als je data verwerkt of doorgeeft buiten de EU GDPR materie contractueel afgedwongen worden.