GDPR op maat van je sportfederatie

Vlaamse Sportfederatie

Vlaamse Sportfederatie vzw

19-3-2018

GDPR op maat van je sportfederatie

In regel met de privacywetgeving in 8 stappen

1. Algemeen

Vanaf 25 mei 2018 moet de Europese Verordening rond GDPR (of General Data Protection Regulation) toegepast worden. Deze Europese uniformisering van de privacywetgeving op het vlak van verwerking en bescherming van persoonsgegevens zal gevolgen hebben voor zowel grote als kleine organisaties.

Om sportfederaties te ondersteunen, maakten we deze beknopte handleiding op. In combinatie met de tools waarnaar verwezen wordt, moet het je sportfederatie in staat stellen om een GDPR-beleid uit te werken met beperkte administratieve last. Je kan de tools downloaden via www.vlaamsesportfederatie.be/product (trefwoord GDPR).
Voor sportclubs zijn gelijkaardige documenten opgemaakt. Promoot gerust bij jullie clubs het gebruik van deze documenten. Je kan ze downloaden via www.dynamoproject.be/documenten.

2. Begrippen

Volgende begrippen worden in deze handleiding vaak gebruikt, en zijn dus handig om vooraf even door te nemen.

- **Verwerking**: alles wat je kan doen met een (persoons)gegeven, van het verzamelen, raadplegen, verspreiden, koppelen en registreren tot het vernietigen van gegevens
- **Persoonsgegevens**: gegevens over een identificeerbaar natuurlijke persoon zoals naam, adres, geslacht, lichamelijke of psychische kenmerken, geaardheid, vrijetijdsbesteding, opleiding, beroep, prestaties, resultaten, ...
- **Betrokken persoon**: leden, deelnemers, enz. wiens gegevens je verwerkt
- **Verwerkingsverantwoordelijke**: de rechts- of natuurlijke persoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel en de middelen van de verwerking vaststelt.
- **Verwerker**: een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt
- **Derde**: een natuurlijk of rechtspersoon die geen betrokkene, verantwoordelijke of verwerker is. Een derde ontvangt persoonsgegevens van de verwerkingsverantwoordelijke, en kan deze gegevens eventueel zelf verwerken volgens eigen bepalingen (niet volgens jouw instructies)

3. Stappenplan

STAP 1: Bewustmaking

Het implementeren van de GDPR in je sportfederatie begint met een **bewustmaking rond privacy**. Bespreek samen met het bestuur, de vrijwilligers, de medewerkers,… volgende zaken:

- het belang van privacy van je leden en deelnemers
- de stappen die je sportfederatie zal zetten om de vereniging in regel te brengen met GDPR (bv. de stappen in deze handleiding)
- de beveiliging van persoonsgegevens

Hou hierbij steeds de kernprincipes proportionaliteit, legaliteit en transparantie in het oog (zie verder). Documenteer deze fase door dit bv. in verslagen van vergaderingen te vermelden.

STAP 2: Opmaak inventaris (+ tool)

De GDPR-wetgeving leidt er niet toe dat je plots geen gegevens meer mag bijhouden. Wel is het belangrijk dat je kunt aantonen waarom je bepaalde gegevens opvraagt, waarvoor je ze gebruikt,... Het proportionaliteitsprincipe dient daarbij te worden gerespecteerd. Dit betekent dat enkel noodzakelijke persoonsgegevens opgevraagd en verzameld mogen worden. De gegevens mogen bewaard worden zolang dit nodig is, zolang je maar argumenteert/documenteert waarom die bepaalde termijn nodig is. Beperk ook de personen die toegang hebben tot de gegevens tot diegene die dit strikt gezien nodig hebben.

Aan de hand van de tool **"**inventaris gegevensverwerking" kan je een goed zicht krijgen op de gegevensverwerking in je sportfederatie. De tool omvat een vragenlijst waarmee je een inventaris van de gegevenswerking in je sportfederatie opmaakt. De wetgeving verplicht je sportfederatie niet tot de opmaak van zo'n inventaris of beginsituatie, maar het is wel een handig hulpmiddel als voorbereiding op de opmaak van het verplichte register van gegevensverwerking (stap 4, zie verder).

STAP 3: Toetsing GDPR (+ tool)

Nadat je de inventaris opgemaakt hebt, kan je nagaan hoever je staat met de bescherming van de privacy van je leden en deelnemers. Hierbij is het belangrijk om rekening te houden met het legaliteitsprincipe. Let er onder meer op dat je:

- iedereen duidelijk **informeert** (bv. via een privacyverklaring, zie verder)
- een **wettelijke grond hebt om gegevens te verwerken**. Er zijn zes rechtsgronden opgenomen in de GDPR- Verordening (zie hieronder)
- **enkel de nodige gegevens** opvraagt en deze **niet langer bewaart dan nodig** is
- de gegevens voldoende **beveiligt**
- iedere betrokken persoon de **mogelijkheid geeft zijn/haar rechten uit te oefenen**, onder andere om hun gegevens in te zien, te corrigeren, te laten verwijderen, enz.

Rechtsgronden voorzien in de GDPR verordening

1. **Contractuele grond**: de verwerking is noodzakelijk voor de uitvoering van een overeenkomst (bv. een vrijwilligersovereenkomst, een lidmaatschapsovereenkomst, deelname-overeenkomst,…).
2. **Gerechtvaardigd belang**: de verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde. Zoniet is de activiteit niet uitvoerbaar. Er moet wel een afweging gemaakt worden, met name of het gerechtvaardigd belang zwaarder doorweegt dan de rechten of vrijheden die de betrokkenen hiervoor moeten inleveren (bv. het aanbieden en organiseren van sport).
3. **Wettelijke verplichting**: de verwerking is noodzakelijk om te voldoen aan een wettelijke verplichting, bvb subsidiewetgeving.
4. **Toestemming**: je hebt ondubbelzinnige en expliciete toestemming verkregen van de persoon. Je hebt deze toestemming dus door een actie van de betrokken persoon gekregen.
5. Vitaal belang: de verwerking is noodzakelijk om de vitale belangen van de betrokkene of andere natuurlijke personen te beschermen (bv. omwille van een dringende medische reden)
6. Algemeen belang: de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen (bv. politie)

De eerste vier rechtsgronden (contractuele grond, gerechtvaardigd belang, wettelijke verplichting en toestemming) kunnen van toepassing zijn in de context van een sportfederatie. De twee laatste rechtsgronden (vitaal belang en algemeen belang) zijn normaal gezien niet van toepassing voor je sportfederatie.

Aan de hand van tool **"**toetsing GDPR**"** kan je nagaan hoever je staat met de bescherming van de privacy van je leden en deelnemers. Net zoals de eerste tool, wordt deze tweede tool niet verplicht vanuit de wetgeving.

STAP 4: Register van gegevensverwerking (+ tool)

De GDPR-wetgeving stelt dat je sportfederatie een register van gegevenswerking moet opmaken. In het register houdt de verwerkingsverantwoordelijke (met name je sportfederatie) onder meer de verwerkingsdoeleinden, de categorieën van ontvangers van de persoonsgegevens, enz. bij.

Door de eerste twee tools te gebruiken ("Inventaris gegevensverwerking" en "toetsing GDPR"), heb je al heel wat input verzameld voor het invullen van het register van gegevensverwerking.

In de tool **"**Register van gegevensverwerking**"** vul je per soort activiteit die je sportfederatie verricht (ledenbeheer, organiseren van activiteiten,…) alle gevraagde informatie in. Dit register is een verplicht document en vormt dus één van de essentiële onderdelen van een goed GDPR-beleid. De tool is een Excel-bestand. In het eerste tabblad vind je een handleiding die je wegwijs maakt in het gebruik van de tool.

STAP 5: Privacyverklaring (+ tool)

De GDPR-Verordening verplicht de gegevensverantwoordelijke om, overeenkomstig het transparantieprincipe, op een beknopte, open , begrijpelijke en gemakkelijk toegankelijke vorm én in duidelijke en eenvoudig taal, de betrokkene te informeren over volgende zaken:

- Welke gegevens worden verwerkt?
- Waar verzamelt je sportfederatie de gegevens?
- Waarom worden de gegevens bewaard?
- Wie verwerkt buiten je organisatie de gegevens?
- Wie krijgt de gegevens?
- Wat wordt precies hoe, waar en hoelang bewaard?
- Hoe worden je gegevens beveiligd?
- Hoe zorg je voor de uitoefening van de rechten van betrokken personen?

Deze informatie wordt verplicht gebundeld in een privacyverklaring die op de website van de sportfederatie wordt gepubliceerd. Je kan vanuit andere documenten (zoals een lidmaatschapsformulier, deelnemersinschrijving, enz.) via een korte verklaring verwijzen naar de uitgebreide privacyverklaring. Vermeld in de verkorte verklaring wel welke gegevens je voor die actie (bv. een ledenregistratie) opvraagt en hoe je ze beschermt en bewaart.

Een privacyverklaring moet niet goedgekeurd worden. Het gaat om eenzijdige verklaring van een organisatie waarin ze bepaalt hoe er met de persoonsgegevens zal worden omgegaan. Enige uitzondering hierop is de verwerking van gegevens op basis van de rechtsgrond toestemming.

Het is belangrijk om op te merken dat de informatie proactief moet verstrekt worden. Je sportfederatie dient de privacyverklaring dus te bezorgen vooraleer de persoonsgegevens verwerkt worden.

In de tool **"**Model privacyverklaring**"** vind je een model dat je kan aanpassen naar de noden van je sportfederatie.

STAP 6: Antwoorden op vragen van betrokkenen

De betrokkenen in je sportfederatie hebben verschillende rechten. Als een betrokken persoon je sportfederatie een vraag stelt op basis van zijn rechten, moet je sportfederatie hier een correct gevolg kunnen aan geven . Volgende rechten van de betrokkene staan uitgeschreven in de artikelen 13 tot 22 van de GDPR-Verordening:

- **Recht op informatie**: de betrokkene heeft recht op het verkrijgen van bepaalde informatie zoals onder meer de identiteit en contactgegevens van de verwerkingsverantwoordelijke, de verwerkingsdoeleinden, de rechtsgrond, enz.
- **Recht op inzage en kopie**: de betrokkene heeft het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken van zijn/haar persoonsgegevens, en om in zijn/haar gegevens inzage te krijgen. Daarnaast mogen onder meer ook de verwerkingsdoeleinden, de betrokken categorieën van persoonsgegevens, de ontvangers, de duur van het bijhouden van de gegevens, enz. opgevraagd worden. Ook een kopie van alle op hem/haar betrekking hebbende gegevens kan kosteloos opgevraagd worden.
- **Recht op aanpassing**: de betrokkene heeft het recht om aan de verwerkingsverantwoordelijke te vragen om onjuiste persoonsgegevens recht te zetten.
- **Recht op bezwaar**: de betrokkene heeft het recht om bezwaar te maken tegen de verwerking van hem of haar betreffende persoonsgegevens. De verwerkingsverantwoordelijke staakt de verwerking tenzij hij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene.
- **Recht op verwijdering (om vergeten te worden):** de betrokkene heeft onder bepaalde voorwaarden het recht om te vragen dat zijn/haar gegevens gewist worden.
- **Recht op intrekken van toestemming**: wanneer de verwerking van de persoonsgegevens gebaseerd was op de rechtsgrond toestemming van de betrokkene, kan de betrokkene deze toestemming steeds intrekken.
- **Recht op overdraagbaarheid**: de betrokkene heeft het recht om zijn/haar persoonsgegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij gehinderd te worden door de verwerkingsverantwoordelijke aan wie de persoonsgegevens waren verstrekt.
- **Recht op weigering geautomatiseerde individuele besluitvorming, profilering:** de betrokkene heeft het recht om niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerde besluitvorming waaraan voor hem/haar rechtsgevolgen zijn verbonden of dat hem/haar aanzienlijk treft.
- **Recht op beperking van de verwerking: in bepaalde gevallen** (bv. een onrechtmatige verwerking waarbij de betrokkene zich verzet tegen het wissen van de persoonsgegevens,…) heeft de betrokkene het recht om van de verwerkingsverantwoordelijke de beperking van de verwerking te verkrijgen.

In de privacyverklaring (zie stap 5) worden al deze rechten van de betrokkene toegelicht.

STAP 7: Contracten verwerkingsverantwoordelijke – verwerker (+ tool)

Vaak blijven persoonsgegevens niet binnen één organisatie, maar worden de gegevens aan andere organisaties doorgegeven om daar te worden verwerkt volgens de instructies van de verantwoordelijke. Op dat moment ontstaat er een relatie tussen de “verwerkingsverantwoordelijke” en de “verwerker” (zie “Begrippen” voor verklaring van de begrippen). Als sportfederatie geef je bv. gegevens door aan je informaticadienstverlener of cloud-provider. Het is dan ook van belang dat elk van de organisaties waarmee je contracteert, de gegevensverwerking op een correcte manier verricht.
Wanneer een verwerker een verwerking namens een verwerkingsverantwoordelijke verricht, dan zorgt de verwerkingsverantwoordelijke ervoor dat hij voldoende garanties heeft dat de verwerker zelf ook de GDPR zal respecteren. De verwerker zal dus zelf ook passende technische en organisatorische maatregelen moeten kunnen bieden.
De verwerkingsverantwoordelijke en verwerker moeten zich aan de hand van een overeenkomst verbinden tot het naleven van de GDPR. Een model van dergelijke verwerkersovereenkomst vind je in de tool **“**Modelcontract verwerkingsverantwoordelijke – verwerker”.

STAP 8: Aanpak datalek (+ tool)

Als er zich binnen je sportfederatie een verlies van persoonsgegevens voordoet, spreekt men van een datalek. Dit kan onder meer gebeuren wanneer er een laptop wordt gestolen, wanneer je computer wordt gehackt, wanneer je een usb-stick met alle adressen van de leden verliest, enz.
Je moet als organisatie een intern bestand bijhouden met alle incidenten van mogelijke lekken van gegevens.

Bij een datalek moet je de Gegevensbeschermingsautoriteit, de vroegere Privacycommissie, (Drukpersstraat 35, 1000 Brussel, www.gegevensbeschermingsautoriteit.be) inlichten binnen de 72 uur na vaststellen van het datalek, tenzij het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Niet naleven van de meldplicht bij een datalek kan stevige boetes met zich meebrengen.

Bij een hoog risico voor de rechten en vrijheden van de betrokkene, moet dit ook aan de betrokkene zelf meegedeeld worden, zodat de nodige voorzorgsmaatregelen genomen kunnen worden.

De tool **"**aangifteformulier datalek**"** biedt een model dat je sportfederatie kan helpen om een aangifte van een datalek te doen.

STAP 9: Afweging verplichting DPO

Sommige organisaties worden door de GDPR verordening verplicht om een een functionaris voor gegevensbescherming aan te stellen, ook wel de Data Protection Officer (kort: DPO) genoemd. De DPO moet de organisatie bijstaan bij het toezicht op de interne naleving van de GDPR binnen de organisatie (een soort preventieadviseur voor privacy).

Moet ik als sportfederatie een DPO aanstellen?

Er zijn drie situaties waarin de GDPR de aanstelling van een DPO verplicht aan organisaties:

1. Overheidsinstantie
2. "Bent u hoofdzakelijk belast met het verwerken van persoonsgegevens die regelmatige en stelselmatige observatie op grote schaal eisen?"
3. "Bent u hoofdzakelijk belast met het verwerken van gevoelige gegevens"

Situatie 1 is sowieso niet van toepassing.
Situatie 2 kan eventueel van toepassing zijn indien je sportfederatie een significant deel van de werking spendeert aan profiling ed, maar de kans is eerder klein. Situatie 3 lijkt enkel van toepassing op een aantal specifieke federaties (denk aan gehandicaptensport, schietsport,…). Hierbij is het belangrijk dat elke federatie in een zeer beperkte mate over gevoelige gegevens kan beschikken (vanuit topsport bvb) zonder per definitie onder de DPO verplichting te vallen. In dat geval is de "hoofdzakelijk" niet van toepassing. Dat neemt niet weg dat in elk geval (los van de verplichting om al dan niet een DPO te hebben) ALLE gevoelige gegevens in de federatie extra moet beschermen (beveiligen via paswoorden, encrypteren, regelmatig verwijderen, etc).

Twijfel je of jouw sportfederatie tot situatie 1 of 2 behoort? Of twijfel je niet maar wil je voor de zekerheid een document om de beslissing te staven? Via de tool **"Evalutie DPO verplichting" (nog in ontwikkeling)** kan je een aantal zaken op een rijtje zetten en op basis daarvan "concluderen" of je wel of geen DPO nodig hebt.