



dynamoproject.be

# Handleiding GDPR op maat van je sportclub

Versie 2 – mei 2018

© Vlaamse Sportfederatie vzw



Dynamo Project  
is een project van   
Vlaamse Sportfederatie

 **SPORT.**  
VLAANDEREN

# GDPR op maat van je sportclub

## In regel met de privacywetgeving in 8 stappen

Deze handleiding kwam tot stand in samenwerking met Scwitch en T&C Blue Horizon.

### 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 sportclubs te ondersteunen, maakten we deze beknopte handleiding op. In combinatie met de tools waarnaar verwezen wordt, moet het je sportclub in staat stellen om een GDPR-beleid uit te werken met beperkte administratieve last. Je kan de tools downloaden via [www.dynamoproject.be/documenten](http://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.
- **Derde-verwerker:** een natuurlijke of rechtspersoon, een overheidsinstantie, een dienst of ander orgaan die/dat op instructie van de verwerkingsverantwoordelijke persoonsgegevens verwerkt
- **Derde-ontvanger:** 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 de instructies van de verwerkingsverantwoordelijke)

### 3. Stappenplan

STAP 1 BEWUSTMAKING

STAP 2 OPMAAK INVENTARIS (TOOL 1)

STAP 3 TOETSING GDPR (TOOL 2)

STAP 4 REGISTER VAN GEGEVENSVERWERKING  
(TOOL 3)

STAP 5 PRIVACYVERKLARING (TOOL 4)

STAP 6 ANTWOORDEN OP VRAGEN VAN  
BETROKKENEN

STAP 7 RELATIES MET DERDEN (TOOL 5)

STAP 8 AANGIFTE DATALEK (TOOL 6)

## STAP 1: Bewustmaking

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

1. het belang van privacy van je leden en deelnemers
2. de stappen die je sportclub zal zetten om de vereniging in regel te brengen met GDPR (bv. de stappen in deze handleiding)
3. 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

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 "[Tool 1: Opmaak inventaris](#)" kan je een goed zicht krijgen op de gegevensverwerking in je sportclub. De tool omvat een vragenlijst waarmee je een inventaris van de gegevensverwerking in je sportclub opmaakt. De wetgeving verplicht je sportclub 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

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:
  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, bv. 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 sportclub. De twee laatste rechtsgronden (vitaal belang en algemeen belang) zijn normaal gezien niet van toepassing voor je sportclub.

- 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.

Aan de hand van "[Tool 2: 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

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

Het is belangrijk op te merken dat het register voor intern gebruik moet opgemaakt worden. Je hoeft het dus niet naar een bepaalde instantie op te sturen. Het is wel mogelijk dat de Gegevensbeschermingsautoriteit bij een controle het register wil kijken.

Door de eerste twee tools te gebruiken ("Tool 1: Opmaak inventaris" en "Tool 2: Toetsing GDPR"), heb je al heel wat input verzameld voor het invullen van het register van gegevensverwerking.

In "[Tool 3: Register van Gegevensverwerking](#)" vul je per soort activiteit die je sportclub 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

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

- Welke gegevens worden verwerkt?
- Waar verzamelt je sportclub 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 sportclub 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 sportclub dient de privacyverklaring dus te bezorgen vooraleer de persoonsgegevens verwerkt worden.

In "[Tool 4: Privacyverklaring](#)" vind je een model dat je kan aanpassen naar de noden van je sportclub. Let erop dat de informatie uit het verwerkingsregister overeenstemt met de informatie uit de privacyverklaring.

## STAP 6: Antwoorden op vragen van betrokkenen

De betrokkenen in je sportclub hebben verschillende rechten. Als een betrokken persoon je sportclub een vraag stelt op basis van zijn rechten, moet je sportclub 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 uitsluitend 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 vergete 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: Relaties met derden

Vaak blijven persoonsgegevens niet binnen één organisatie, maar worden de gegevens aan andere organisaties (derden) doorgegeven. Indien dit het geval is, moet dit in de privacyverklaring opgenomen worden. Afhankelijk van het type derde (derde-verwerker of derde-ontvanger), moet je met volgende zaken rekening houden.



## Derde-verwerker

In het geval dat je sportclub persoonsgegevens doorgeeft aan derden die deze verder verwerken volgens jouw instructies, spreek je over een “derde-verwerker.” Verwerken moet ruim geïnterpreteerd worden: in geval van louter stockeren van persoonsgegevens in opdracht van een organisatie is er al sprake van verwerken. Een voorbeeld van een verwerker is een ICT partner of cloud-provider.

Wanneer een verwerker dus op jouw instructie persoonsgegevens verwerkt, dan moet je een verwerkingsovereenkomst afsluiten:

Er zijn verschillende mogelijkheden om zo'n overeenkomst vorm te geven.

1. Bij contracten met ondernemingen kunnen afspraken rond privacy opgenomen worden in de algemene verkoops- of gebruiksvoorwaarden. Van de meeste grote ondernemingen mag je verwachten dat ze zelf initiatief nemen om hun voorwaarden aan te passen en hun klanten te contacteren om de aangepaste voorwaarden te aanvaarden (actief akkoord is vereist).
2. Specifiek voor de relatie tussen een federatie en zijn leden/clubs kunnen afspraken rond het gebruik van persoonsgegevens ook opgenomen worden in interne reglementen (huishoudelijk reglement, toetredingsformulier, enz.). Het heeft weinig toegevoegde waarde voor een federatie om met elke club afzonderlijk een contract te gaan beheren, maar er moeten wel duidelijke afspraken zijn. De federatie neemt dus best een passage op in een intern reglement waarin de relatie tussen beide organisaties en hun wederzijdse rechten en plichten rond privacy worden beschreven. Federaties en hun nationale en internationale koepel kunnen het ook op deze manier vormgeven. Deze aanpassing in de interne reglementen hoeft niet actief goedgekeurd te worden door de leden, gezien het statutair bepaald is dat de leden de interne reglementen dienen na te leven. Wel moet er duidelijk over gecommuniceerd te worden zodat iedereen op de hoogte is van de aanpassingen.
3. In eventuele overblijvende gevallen (geen initiatief van de leverancier in aanpassing van de voorwaarden) kan ons model van verwerkersovereenkomst “Tool 5: Modelcontract verwerkingsverantwoordelijke – verwerker” gebruikt worden.

## Praktisch

Het Dynamo Project neemt het initiatief om namens de georganiseerde sportsector een aantal grote en veel gebruikte verwerkers in de sportsector te contacteren en in kaart brengen in welke mate ze in orde zijn met de GDPR regelgeving. Een stand van zaken kan je terugvinden in deze [FAQ](#).

Voor de overige verwerkers die zelf geen initiatief nemen om een overeenkomst (onder de vorm van aangepaste voorwaarden of een contract) op te maken, raden we aan om zelf contact op te nemen op basis van het voorbeeldmailtje hieronder en om vervolgens de instructies of stappen die de onderneming voorstelt te volgen of zelf een modelovereenkomst voor te stellen indien dit niet voldoende lijkt.

Voorbeeldmailtje naar verwerkers:

*“In het kader van de implementatie van GDPR binnen onze organisatie, werd uw onderneming/organisatie aangemerkt als verwerker van persoonsgegevens waarvoor wij verantwoordelijk zijn. Volgens artikel 28 AVG dienen wij voor elke verwerker na te gaan of deze de GDPR verplichtingen zal naleven (en dus GDPR compliant is).*

*Kan u daarom per kerende bevestigen dat uw organisatie GDPR compliant is, en met name volgende principes worden gerespecteerd:*

- *Dat wij eigenaar zijn van de gegevens en dat uw onderneming/organisatie deze gegevens niet zal*





delen met andere partijen of voor eigen doeleinden kan gebruiken

- Dat de verstrekte persoonsgegevens binnen Europa blijven, en op Europese dataservers worden gestockeerd
- Dat de gegevens afdoende beveiligd zijn
- Dat de gegevens vertrouwelijk worden behandeld (o.a. door uw medewerkers en leveranciers)

Kan u mij ook laten weten op welke manier u deze informatie schriftelijk zal vastleggen, mogelijks via een uitbreiding van een gebruikersovereenkomst of verkoopsvoorwaarden?"

### Derde-ontvanger

In het geval dat je gegevens doorgeeft aan een derde die ze niet verder op jouw instructie verwerkt, dan spreek je over een "derde-ontvanger". Op dat moment moet je als club bewijs kunnen leveren dat je weet dat deze derde op een veilige manier zal omgaan met de gegevens (je kan hiervoor onderstaand kort voorbeeldmailtje gebruiken).

Voorbeeldmailtje naar ontvanger:

*"In het kader van de implementatie van GDPR binnen onze organisatie, werd uw onderneming/organisatie aangemerkt als ontvanger van persoonsgegevens waarvoor wij verantwoordelijk zijn.*

*Kan u daarom per kerende bevestigen dat uw organisatie GDPR compliant is en u bijgevolg op een veilige manier met de doorgegeven gegevens zal omgaan?"*

Om de relaties met derden goed op te volgen, wordt best een lijst van derden (verwerkers en ontvangers) opgemaakt waarin wordt bijgehouden of de organisatie in kwestie al GDPR-compliant is en op welke manier de onderlinge afspraken geregeld zijn (contract, voorwaarden, enz.)

## STAP 8: Aanpak datalek

Als er zich binnen je sportclub 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](http://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.

In "[Tool 6: Datalek](#)" vind je een model dat je sportclub kan helpen om een aangifte van een datalek te doen.