FAQ's rond GDPR

In deze FAQ's trachten we eenvoudige antwoorden te geven op vragen die we geregeld ontvangen rond GDPR voor socioculturele organisaties. Op de meeste vragen kunnen we een duidelijk antwoord geven. Sommige vragen zijn echter afhankelijk van de aard van uw organisatie (vb de keuze van de wettelijke gronden). Daar trachten we vooral de geest van de GDPR duidelijk te maken, zodat u hier verder mee aan de slag kan. Meer info, tools en templates vind je op scwitch.be/toolkit bij 'GDPR' en 'GDPR' lokale verenigingen.

scwitch
ZAKELIJK ORGANISATIEMANAGEMENT

Moet mijn organisatie zich in regel stellen met de GDPR?

JA

Elke organisatie, zowel vzw's als feitelijke verenigingen, moet tegen 25 mei 2018 in regel zijn met de GDPR verordening. De GDPR is ontwikkeld om de persoonsgegevens van individuen te beschermen en is eigenlijk gewoon een aanpassing van de vroegere privacywetgeving.

De GDPR is dus ook van toepassing op het lokale verenigingsleven. Het is ook logisch dat elke organisatie de privacy van zijn leden, deelnemers,… respecteert. Het bezorgt organisaties wel extra werk. De gratis scwitch modeldocumenten en templates proberen het werk wat te verlichten.

Elke organisatie is verantwoordelijk voor het gebruik van persoonsgegevens en moet steeds kunnen aantonen hoe de organisatie dit aanpakt (accountability principe = 'verantwoording' maar ook 'verantwoordelijkheid')

Wat betekent dit?

- je organisatie neemt zelf initiatief om zich in regel te brengen met de GDPR en wacht niet tot er zich een probleem stelt
- je organisatie houdt al de stappen die ze neemt goed bij

Wat moet mijn organisatie doen om zich in regel stellen met de GDPR?

drie sleutelwoorden: **informeren / documenteren / beveiligen**

Informeren

Elke organisatie moet zijn leden, deelnemers aan activiteiten, partner,… wiens persoonsgegevens hij gebruikt (opslaan, bewaren, publiceren, doorgeven…) goed informeren over waarom je welke gegevens gebruikt.

Je informeert in een duidelijke taal, bij het eerste moment waarop je gegevens opslaat. Voor verenigingen is dit meestal bij inschrijving als lid of deelname aan een activiteit. Als je een website hebt, maak je best een privacyverklaring op waarnaar je kan verwijzen op je deelnemings- of inschrijvingsformulieren. We raden je aan om op je deelnemers- of inschrijvingsformulieren ook kort te vermelden waarom je de gegevens opvraagt en hoe je hier mee omgaat. Als je toestemming vraagt voor het gebruik van gegevens, doe je dit ook op het allereerste moment dat mensen je hun gegevens bezorgen. De toestemming geldt enkel voor de doeleinden waarvoor je deze toestemming vraagt.

Documenteren

GDPR is een zaak van iedereen in je organisatie die persoonsgegevens kan zien of gebruikt. Handel dit niet alleen af. Betrek alle medewerkers van je organisatie hierbij.

Je moet elke stap die je zet en elke beslissing die je neemt goed documenteren en bijhouden. Hou alles over je aanpak van privacy van je deelnemers, leden, … goed bij.

Maak hiervoor gebruik van een duidelijk register (meer info : zie register) . Elke organisatie is trouwens verplicht een register bij te houden (lidmaatschap, activiteiten, nieuwbrief).

Beveiligen

Elke organisatie is verantwoordelijk voor het gebruik van persoonsgegevens van zijn leden. Dit betekent dat je er ook zorgzaam moet mee omgaan. Door de gegevens te beveiligen. We geven alvast een aantal tips

- Gegevens die je eigenlijk niet (meer) nodig hebt, schrap je direct.
- Laat geen lijsten rondslingeren en maak hier duidelijke afspraken rond met je mede vrijwilligers, leiding, bestuur,…
- Versleutel. Dit gaat van het bewaren van medische fiches in een gesloten koffertje, tot bewaren van documenten op laptops.
- zet niet zomaar foto’s op het net. Plaats ze in afgeschermde omgevingen en zorg er voor dat beeldmateriaal niet zomaar kan van het net gehaald worden.

Wat zijn de verplichtingen binnen de GDPR?

- Je moet een **register** van gegevensverwerking maken en bijhouden voor alle categorieën van gegevensverwerking binnen je organisatie. Eventueel gebruik je hiervoor de scwitch templates voor register ledenregistratie en register activiteitenregistratie.

- Je moet een **privacyverklaring** hebben waarin je iedereen duidelijk en actief informeert over het gebruik van hun persoonsgegevens binnen je organisatie. Kijk of je koepel of federatie kan helpen met de opmaak van een privacyverklaring.

- Je moet gegevens goed beveiligen en hier **organisatorische** (paswoorden,…) en **technische** (antivirussoftware) **maatregelen** rond nemen.

- Je moet kunnen **reageren op vragen** van leden, deelnemers, partners,… rond het gebruik van hun persoonsgegevens.

- je moet snel en efficiënt kunnen reageren in geval van een **datalek** (aangeven binnen de 72u na ontdekking)

- je moet duidelijke **overeenkomsten** hebben dat organisaties of **partners** die voor jou gegevens verwerken ook werken volgende de regels van GDPR

- Je moet ook volgende basisprincipes respecteren:
  - **legaliteit:** je moet duidelijk bepalen en meedelen op basis van welke wettelijke gronden je persoonsgegevens verwerkt
  - **proportionaliteit:** je mag enkel de hoogstnoodzakelijke persoonsgegevens opvragen en verwerken. Je mag de gegevens enkel zo lang als noodzakelijk bijhouden.
  - **transparantie:** de betrokkenen moeten duidelijk geïnformeerd worden over het gebruik van hun gegevens (zie ook privacyverklaring)

Hoe pak ik dit aan?

Ga planmatig te werk en houd alles goed bij

De GDPR-verordening is geen zwart-wit regelgeving. Je hebt de ruimte om als organisatie keuzes te maken, zoals bijvoorbeeld bij de wettelijke grond om persoonsgegevens te gebruiken. Denk hier over na, maak duidelijke keuzes, informeer je leden, deelnemers,… hier goed over en motiveer duidelijk je keuzes in een intern document

Ook bij beveiliging en de diverse stappen die je organisatie misschien nog moet zetten om 100% in regel te zijn, is het belangrijk om goed na te gaan wat de grootste en dringendste problemen zijn. Wat zijn de grootste risico's? Wat is het snelst haalbaar? Wat is dringend en noodzakelijk? Waar moet je nog stevig in investeren. (en pak je nog na 25 mei verder aan…)

Maak op basis van die oefening een realistische planning. 25 mei 2018 is de deadline. tegen dan heb je best een register, duidelijke privacyverklaring en sta je klaar om potentiële vragen van betrokkenen te kunnen beantwoorden. Zijn er daarnaast zaken die je nog niet kan realiseren, zet dan in op de hoogste noden en prioriteiten, plan een realistisch en aanvaardbaar vervolg, argumenteer en documenteer dit

.

in het scwitch logboek stellen we volgende stappenplan voor:

1. **bewustwording**: agendeer het thema op je bestuur
2. **inventariseer**: lijst op wie welke gegevens waar, waarom en voor hoe lang bewaart
3. **onderzoek** volgende zaken:
    1. heb je alle gegevens nodig?
    2. (hoe) beveilig je de persoonsgegevens?
    3. op basis van welke wettelijke grond bewaar je gegevens
4. Maak een r**egister** op voor elke vorm van gegevensregistratie (vb ledenregistratie, organisatie van activiteiten,…)
5. maak een goede **privacyverklaring** op (op basis van je inventaris en register)
6. werk **procedures** uit zodat je de r**echten van betrokkenen** kan respecteren
7. werk een **procedure** uit zodat je kan reageren in geval van een **datalek**

Wat is een goede privacyverklaring?

Als verwerkingsverantwoordelijke moet je organisatie de betrokkenen pro-actief en duidelijk informeren over watje met de persoonsgegevens van leden, deelnemers,… doet en wat hun rechten zijn.

Dit moet beknopt, transparant, in een duidelijke eenvoudige taal en in een begrijpelijke en gemakkelijk toegankelijke vorm. Door de opmaak van een heldere en makkelijk raadpleegbare privacyverklaring voldoe je duidelijk aan deze verplichting.

Opgelet: je maakt de privacyverklaring op in functie van de categorie betrokkenen waar je je toe richt (leden, deelnemers werknemers, kinderen…). De inhoud en locatie waarop je de privacyverklaring meedeelt hangen dus ook af van deze categorie.

Je privacyverklaring zet je raadpleegbaar op de meest aangewezen plaats voor de betrokkenen van wie de persoonsgegevens verwerkt worden. Dit betekent: je website voor leden, de algemene voorwaarden van het lidmaatschaps- of deelnemersformulier, vrijwilligersnota,…

Moet ik steeds de volledige privacyverklaring meegeven?

Neen. Als je privacyverklaring duidelijk op je website staat, mag je hier naar verwijzen op je andere documenten. We raden je wel aan om op de andere documenten beknopt mee te delen wat je beleid is rond privacy en gebruik van persoonsgegevens, waarna je specifiek doorverwijst naar de volledige privacyverklaring.

Welke zaken neem je op in je privacyverklaring

- WELKE gegevens worden verwerkt?
- WAAR krijgt of verzamelt je organisatie de gegevens?
- WAAROM worden de gegevens bewaard?
- WIE verwerkt in je organisatie gegevens?
- WIE krijgt de gegevens?
- WAT wordt precies HOE, WAAR en HOELANG bewaard?
- HOE worden gegevens beveiligd?
- HOE faciliteer je de uitoefening van de rechten van betrokkenen?

Op basis van welke wettelijke grond mag ik persoonsgegevens verwerken.

Er zijn 6 wettelijke gronden op basis waarvan je persoonsgegevens mag verwerken. Van die 6 zijn er vier mogelijke toepasbaar voor je organisatie. Het is aan jouw organisatie om de keuze te maken, dit te motiveren en je leden, deelnemers hierover te informeren (in je privacyverklaring).

- **wettelijke verplichting**
- **contractuele basis**
- **ondubbelzinnige toestemming**
- **gerechtvaardigd belang**

wettelijke verplichting (noodzakelijk voor de uitvoering van een wettelijke plicht)
De verwerking van gegevens is opgelegd door een wet, decreet,… Voor deze wettelijke grond is er geen toestemming nodig. Je moet de personen wel informeren.

Vaak vraagt de overheid gegevens op als voorwaarde, bewijs voor subsidiedossiers. De voorwaarden zijn in dat geval opgenomen in een gemeentelijk besluit, gemeenteraads- of collegebeslissingen. Meestal vragen overheden geanonimiseerde of gepseudonimiseerde gegevens op, zodat de persoonsgegevens niet meer herkenbaar zijn of terug te brengen zijn tot de specifieke personen in kwestie.
Ook lokale overheden zijn gebonden aan de algemene principes van minimalisatie van gegevens wat betekent dat ze enkel de noodzakelijke gegevens mogen opvragen in verhouding waar het toe dient. schepencolleges hebben dus geen disproportionele macht over het verzamelen van gegevens.

contractuele basis (noodzakelijk voor de uitvoering van een overeenkomst)
Je mag gegevens opvragen als deze noodzakelijk zijn voor de uitvoering van een overeenkomst.
Je hebt bijvoorbeeld iemand zijn naam nodig om hem in te schrijven voor een activiteit.
Er is voor deze grond geen toestemming nodig. Je moet de personen wel informeren.

We veronderstellen dat je het lidmaatschap ook als een vorm van contract mag zien. Zo heb je een minimum aan gegevens nodig van je leden om hem/haar als lid te registeren, en bijvoorbeeld te verzekeren. Je kan deze gegevens opvragen op basis van de grond ‘uitvoering van overeenkomst’. Je moet voor deze gegevens geen goedkeuring vragen, maar het lid hier goed over informeren en de gegevens enkel hiervoor gebruiken.
Let wel: als je dit toepast kan je dit enkel doen voor het minimum aan gegevens noodzakelijk voor registratie lidmaatschap, deelname aan activiteiten.

Gerechtvaardigd belang (de activiteit is anders niet uitvoerbaar)
Dit mag je enkel toepassen wanneer het belang zwaarder doorweegt dan het belang , de rechten en de redelijke privacyverwachting van de betrokkenen.
Het gerechtvaardigd belang biedt wel mogelijkheden, maar je moet als organisatie steeds goed nadenken of je hierdoor voldoet aan de verwachtingen van je leden, deelnemers en je hun privacy niet schendt. Zo kan je als organisatie beslissen dat het noodzakelijk is dat je (geëngageerde) leden (bestuursleden,leiding,…) op de hoogte blijven van je waarden, visie en werking en je hen daarom geregeld informeert via mailings of nieuwsbrieven. Dat kan, maar dan moet je dit goed argumenteren waarom je meent dat je van uit het gerechtvaardigd belang de privacy van je leden, deelnemers beperkt, moet je zeker zijn dat dit binnen hun verwachtingen valt en moet je hen hier goed over informeren. Bij twijfel raden we aan om toch te kiezen voor ondubbelzinnige toestemming.

Ondubbelzinnige toestemming (vrije, actieve en specifieke toestemming van de betrokkenen)

Het vragen van de actieve toestemming is de meest faire en duidelijkste vorm ten opzichte van de betrokkene. Let wel: de toestemming met actief gebeuren: de betrokkenen duidt zelf aan dat hij/zij akkoord gaat. Dit kan niet met op voorhand aangevinkt vakjes of 'uitschrijfmodules'.

We raden dit aan als je als organisatie bijvoorbeeld gsm-nummers van leden, deelnemers, ouders van leden opslaat om hen te kunnen verwittigen bij problemen voor of tijdens een activiteit. Let dat je deze gegevens enkel gebruikt waar je de toestemming hebt voor gekregen, en ze verwijdert zodra ze niet meer nodig zijn. Houdt er rekening mee dat een betrokkene steeds het recht heeft om zijn toestemming in te trekken.