TOOL 2:
Toetsing verwerking persoonsgegevens aan de algemene principes GDPR

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

# Legitimiteit van de verwerking

**Op basis van welke rechtsgronden verwerkt je sportfederatie persoonsgegevens?**

[ ]  de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst**

Zo ja, welk soort overeenkomsten (bv. lidmaatschap):

soort overeenkomst

[ ]  de verwerking gebeurt vanuit een **gerechtvaardigd belang** van de sportfederatie.

*(bv. omdat anders de doelstelling van de sportfederatie niet gerealiseerd kan worden)*

Zo ja, voor welke activiteiten en welke persoonsgegevens:

activiteiten en persoonsgegevens

[ ]  de verwerking is noodzakelijk om te voldoen aan een **wettelijke verplichting**

*(bv. opvragen gegevens voor subsidiedossier voor een overheid)*

Zo ja, op basis van welke wettelijke bepaling en welke persoonsgegevens:

wettelijke bepaling en persoonsgegevens

[ ]  de betrokkene heeft toestemming gegeven

**Vraagt je sportfederatie op een correcte manier toestemming?**

[ ]  je laat vrijwillige keuze

[ ]  je licht ze in over de doeleinden

[ ]  er gebeurt geen stilzwijgende toestemming

[ ]  er is de mogelijkheid tot intrekken van de toestemming

[ ]  de toestemming is controleerbaar

**Vroeg je sportfederatie in het verleden toestemming aan de betrokkenen voor het gebruik van hun persoonsgegevens?**

[ ]  ja
[ ]  neen

# Proportionaliteit

**Waarom houdt je sportfederatie de persoonsgegevens bij?**

*(Je mag enkel persoonsgegevens verzamelen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden.)*

reden verzamelen persoonsgegevens

**Is het noodzakelijk om al deze persoonsgegevens op te vragen, op te slaan en te verwerken voor de beoogde doeleinden van de verwerking?**

*(De persoonsgegevens moeten relevant en beperkt zijn tot de beoogde doeleinden van de verwerking)*

[ ]  ja

[ ]  neen

**Hoelang (hoeveel maanden / jaren of welke periode) houdt je sportfederatie de gegevens bij?**

termijn bijhouden persoonsgegevens

**Worden bestanden, archieven en e-mails regelmatig gewist of opgekuist?**

[ ]  ja

[ ]  neen

**Hoe lang is het noodzakelijk om deze persoonsgegevens te bewaren voor de beoogde doeleinden van de verwerking?**

noodzakelijke termijn bijhouden persoonsgegevens

# Beveiliging en vertrouwelijkheid

Welke **organisatorische maatregelen** treft je sportfederatie om de beveiliging, de vertrouwelijkheid en integriteit van de gegevens te waarborgen zodat ongeoorloofde toegang en gebruik, onopzettelijk verlies, vernietiging, beschadiging of kwaliteitsverlies voorkomen worden? *(bv. Beperkte toegang voor bepaalde personen o.a. door inlogprocedure, gebruik van paswoorden op bestanden…).*

Is men verplicht de wachtwoorden na een bepaalde periode te wijzigen?

[ ]  ja

[ ]  neen

Heeft je sportfederatie een wachtwoordbeleid gecommuniceerd aan de medewerkers, vrijwilligers en partners?

[ ]  ja

[ ]  neen

Zijn er duidelijke instructies naar medewerkers, vrijwilligers en partners over het gebruik van internet, installeren van software, openen van e-mails?

[ ]  ja

[ ]  neen

Communiceert je sportfederatie hier regelmatig over?

[ ]  ja

[ ]  neen

Is er een procedure in geval van datalekken?

[ ]  ja

[ ]  neen

Welke **technische maatregelen** treft je sportfederatie om de beveiliging, de vertrouwelijkheid, en integriteit van de gegevens te waarborgen zodat ongeoorloofde toegang en gebruik, onopzettelijk verlies, vernietiging, beschadiging of kwaliteitsverlies voorkomen worden?

Fysieke beveiliging? fysieke beveiliging.

Hoe vaak neem je back-up van bestanden? regelmaat back-ups.

Op hoeveel verschillende plaatsen worden back-ups bewaard? aantal back-up plaatsen.

Volg je de gevraagde updates van de gebruikte software?

[ ]  ja

[ ]  neen

Gebruik je altijd de laatste versie van de software, toepassingen of apps?

[ ]  ja

[ ]  neen

Maakt je sportfederatie gebruik van cryptografie (encryptie / versleutelen van de gegevens)?

[ ]  ja

[ ]  neen

#  Transparantie

**Heeft je organisatie een privacyverklaring voor elke activiteit waarbij ze persoonsgegevens vraagt aan de betrokkene?**

[ ]  ja

[ ]  neen

Zo ja, welke punten worden erin vermeld:

[ ]  de identiteit van de sportfederatie (naam en adres) en de contactpersoon

[ ]  hoe de informatie wordt verzameld

[ ]  de doeleinden waarvoor de gegevens worden verwerkt (zijn er meerdere, dan moet je ze allemaal toelichten)

[ ]  de wettelijke grondslag voor gegevensverwerking

[ ]  de termijnen waarbinnen de informatie wordt bijhouden

[ ]  of de gegevens aan derden bezorgd worden (en al dan niet uitgewisseld buiten de Europese Unie)

[ ]  de mogelijkheid voor de betrokkene om een klacht in te dienen bij de Gegevensbeschermingsautoriteit (vroegere Privacycommissie) als hij/zij meent dat zijn/haar persoonsgegevens niet correct worden verwerkt

[ ]  de rechten van de betrokkene (bv. recht op toegang en verbetering, recht van verzet,…)

**Krijgt je sportfederatie (indirect) persoonsgegevens van derden?**

[ ]  ja

[ ]  neen

Zo ja, welke en van wie?

welke persoonsgegevens en van wie

Zo ja, worden de betrokkenen (proactief) ingelicht dat deze gegevens werden verkregen?

[ ]  ja

[ ]  neen

**De privacyverklaring (of de plaats waar men ze kan vinden) staat vermeld op:**

[ ]  de website

[ ]  de vrijwilligersnota

[ ]  het lidmaatschapsformulier

[ ]  het inschrijvingsformulier voor deelname aan activiteit

[ ]  andere: andere plaatsen

**Heeft je sportfederatie een intern document waarin haar beleid inzake privacy vastgelegd is (privacy- beleidsplan)?**

[ ]  ja

[ ]  neen