Eglise Protestante Unie de Belgique

Protestant.link

Verenigde Protestantse Kerk in België

Plaatselijke kerk en/of vzw – AVG

1. **Enkele basisbegrippen**

De Europese algemene verordening gegevensbescherming (AVG) is in mei 2018 in voege gekomen en vervangt de Belgische wet inzake de bescherming van het privéleven.
Zij bepaalt op het Europese niveau de regels inzake de bescherming van persoonsgegevens van de Europese burgers

Onder persoonsgegevens dient men alle gevoelige informatie te verstaan die een fysieke persoon rechtstreeks of onrechtstreeks kan identificeren.
Het gaat met name om de naam van de persoon, zijn foto, zijn mutualiteitsnummer, zijn postadres, zijn telefoonnummer, zijn rijksregisternummer, etc.

Indien u meer informatie over de AVG wenst, vindt u hier enkele links ter beschikking

- Voorstelling van de AVG door PRIVACYCOMMISSION.be (FR-versie in het NL ondertiteld)
- De volledige Europese verordening NL - FR - DE
- Artikel per artikel NL - FR - DE

2. **Wat moet u doen?**

De VPKB vraagt elke organisatie om één (1) **gegevensverantwoordelijke** te benoemen, dus een persoon binnen de organisatie die de gegevens in zijn bezit formaliseert.

De secretaris van de kerkenraad of van de bestuursraad lijkt de aangewezen persoon om deze rol in te vullen, maar het kan een andere duidelijk aangewezen persoon zijn.

Deze laatste zal voor iedereen die ernaar vraagt een **register van activiteiten in verwerking (zie model 1)** bijhouden, waarin staat:

· Het soort verwerking
· Het einddoel en de objectieven
· De categorieën van verwerkte gegevens
· De juridische of wettelijke basissen
· De bestemmelingen aan wie de gegevens mogen verschaft worden
· De garanties rond de communicatie van de gegevens aan derden
· De informatiemogelijkheden aan personen waarvan de gegevens worden verwerkt
· De gegevens van een verantwoordelijke bij wie de betrokken personen hun rechten kunnen uitoefenen

· De categorieën van gegevens doorgegeven aan het buitenland, het land van bestemming en de reden voor de uitwisseling
· De geldigheidsduur van de gegevens
· De organisatorische maatregelen en de veiligheidstechnieken

We nodigen alle kerken die een website hebben uit om **het vertrouwelijkheidsbeleid aan te passen/ te kopiëren/ plakken (zie model 2)** op hun website.
Naargelang uw website zal bijkomende informatie ook moeten worden meegedeeld.

3. **Vragen inzake de toestemming**

Artikel 6 (Fr – NL)
Artikel 13 (Fr - NL)

De grote lijnen:
De verwerking van gegevens van persoonlijke aard is enkel mogelijk als de betrokken personen hun toestemming hebben gegeven.
Deze toestemming moet expliciet, duidelijk en **positief** zijn (art. 6, punt 1, a).
Toch wordt de **toestemming** in bepaalde gevallen **verondersteld**. **Wat ons geval is.**
Dit is ook het geval wanneer

- De verwerking nodig is bij de uitvoering van een contract waarvan de betrokken deel uitmaakt (art. 6, punt 1, b);
- De verwerking nodig is voor een juridische verplichting waaraan de gegevensverantwoordelijke onderworpen is (art. 6, punt 1, c). De toestemming wordt ook verondersteld bij een arbeidsovereenkomst, een statuut, het lidmaatschap van een vzw, bijvoorbeeld;
- Ook als men lid wil worden van een vzw als administrator of als lid, moet men de gegevens van persoonlijke aard communiceren als voorzien in de wet van 27 juni 1921.

We merken op dat zelfs in het geval dat de toestemming wordt verondersteld, moeten de betrokken personen ingelicht worden
- over des gegevens van de gegevensverantwoordelijke
- over de gegevens van de afgevaardigde voor de bescherming van gegevens
- over de gegevensbeschermingsautoriteit
- over het einddoel
- over de rechten van de betrokken persoon (art. 13 van de AVG)

(zie model 3)
Elke persoon die in de toekomst aan uw gegevensbestand zal worden toegevoegd en die geen band met de kerk en/of de vzw heeft, zal dus een "toestemmingsformulier" moeten invullen. **(zie model 4)**

4. **Gegevensbescherming**

In verband met artikel 32 zal door elke organisatie een beleid van gegevensbescherming ingevoerd moeten worden. Men moet er eenvoudigweg voor zorgen dat technische en organisatorische maatregelen opgezet worden, die de bescherming van de gegevens voldoende garanderen.