*Grensoverschrijdend gedrag, privacy, fraude en cyberrisks*

# Hoe veilig is jouw kerk?

In Kerkbeheer besteden we geregeld aandacht aan veiligheid in de kerk. In het bijzonder aan de werkomstandigheden (arbo, bhv), als ook aan de veiligheid in de gebouwen (RI&E). Vanzelfsprekend natuurlijk, want kerkrentmeesters hebben een belangrijke opdracht te vervullen om de openbare plek van samenkomst en in hun rol als werkgever te zorgen voor veilige ruimte. Maar veiligheid gaat over meer dan losliggende kabels of een onvoldoende werkplek voor de beheerder. Is het huis ook in overdrachtelijke zin een veilige omgeving en is er voldoende rekening gehouden met dreiging van buitenaf?

**TEKST** JOOST SCHELLING **BEELD** ADOBE STOCK, ISTOCK

## Veilige kerk: het begint bij bewustwording

Veiligheid in de kerk begint met het besef dat (fysiek/financieel/mentaal/seksueel) grensoverschrijdend gedrag overal voorkomt. Sportverenigingen, maatschappelijke organisaties, omroepen, scholen, hulpverlening, families en ook geloofsgemeenschappen. Uit wetenschappelijk onderzoek is bekend, dat in de meeste situaties daders en slachtoffers geen vreemden van elkaar zijn. Reden temeer om juist in de kerk aandacht en oog te hebben voor grensoverschrijdend gedrag en maatregelen te nemen om dit te voorkomen én om adequaat te kunnen reageren als je als geloofsgemeenschap toch met (vermoedens van) grensoverschrijdend gedrag te maken krijgt.

In het kader van voorwaardenscheppende maatregelen heeft de synodevergadering van 21 april 2023 ingestemd met het rapport 'Veilige kerk in de Kerkorde', waarin onder andere kerkordelijk de verplichting tot het aanstellen van een vertrouwenspersoon en het verplicht aanvragen van VOG (Verklaring Omtrent Gedrag) voor ambtsdragers en bepaalde taakdragers in de gemeente vastgelegd zijn. Deze aanpassing in de kerkorde is in 2023 bij classes en gemeente in consideratie gegeven en wordt in 2024 in tweede lezing door de synode vastgesteld.

> "De sleutel ligt bij bewustwording."

In veel kerken zijn al vertrouwenspersonen aangesteld en is het aanvragen van een gratis VOG voor bepaalde vrijwilligers al staande praktijk. Zo ook in de Gereformeerde Kerk Sliedrecht, waar men al in 2020 een projectgroep van de kerkenraad aan het werk zette. Deze projectgroep leverde uiteindelijk een stappenplan tot implementatie van beleid op, maar zorgde vooral ook voor zichtbaarheid van dit traject in de kerkenraad en de gemeente. Inmiddels zijn er twee vertrouwenspersonen aangesteld, zijn er omgangsregels voor het jeugdwerk en de meest kwetsbaren opgesteld, en geldt voor de vrijwilligers een gedragscode.

De predikant, ds. Alexander Veerman, zelf gepromoveerd op seksueel misbruik in de kerk, zegt hierover: "In de periode dat we hieraan gewerkt hebben, zorgde het voor onderling gesprek en bewustwording, want daar begint het mee. Je kunt het zeker niet met afspraken voorkomen, maar het zorgt wel voor een transparantere gemeente, en het besef: 'het kan ook bij ons gebeuren.' Inmiddels zorgen de aangestelde vertrouwenspersonen er ook voor dat het gesprek ook na het beleidsplan op tafel blijft, dat is van groot belang. Trouwens, we gaan ook zorgvuldig naar de vrijwilligers te werk, voor zittende mensen doen we een dringend beroep op het aanvragen van een VOG, voor de nieuwe mensen is het inmiddels onderdeel van de procedure. Zo hopen we iedereen in deze veranderingen mee te nemen." Informatie en procedure over een gratis VOG voor de kerk staat op: www.gratisvog.nl/voorwaarden/preventief-beleid-kerkelijke-organisaties-cio.

## Huis op orde: is persoonlijke en gevoelige informatie in de kerk veilig?

Misschien heeft u zelf wel eens tot frustratie aan toe gehoord: 'nee, ik mag u in het kader van de AVG deze gegevens niet verstrekken.' Dat klinkt soms irritant, maar het voorkomt dat veel van onze meest persoonlijke zaken zomaar op straat komen. Ook kerkgenootschappen vallen onder de Algemene Verordening Gegevensbescherming (AVG). De Protestantse Kerk in Nederland wil bewust en zorgvuldig omgaan met persoonsgegevens en de privacy van haar leden en bezoekers. Daarom is het belangrijk dat iedereen die binnen de kerk met persoonsgegevens te maken heeft zorgt dat hij/zij zich aan de geldende regelgeving houdt. Dat kan gemakkelijk met verschillende modellen en richtlijnen die hiervoor beschikbaar zijn, maar ook hier ligt de sleutel bij de bewustwording. En zeker nu veel van de kerkdiensten online en nog lange tijd terug te vinden zijn. Een paar vuistregels zijn alvast voor veilige omgang te geven:

1. Datgene wat in de openbaarheid over iemand gedeeld wordt, heeft diegene daar ook toestemming voor gegeven? Bekend is het voorbeeld van iemand voor wie met naam en toenaam (en met vermelding op de zondagsbrief) gebeden werd vanwege een psychische aandoening en opname in een kliniek, en dit na jaren nog online terug te vinden was. Het bleek hem bij sollicitaties niet te helpen.
2. Beperk je in de communicatie in de gemeente tot het hoognodige. De kerk is geen roddelblad. De goede verstaander heeft aan een half woord genoeg voor een blijk van medeleven, wie op een nieuwtje uit is, heeft nooit informatie genoeg.
3. Leg vast hoe je met het gebruik van gegevens omgaat, zoals communicatie in je gedrukte media.
4. Zorg dat alles wat je vastlegt, waar het niet je eigen aantekeningen betreft, het daglicht kan verdragen, mocht iemand besluiten zijn wettelijke recht te gebruiken en inzage te vragen wat over hem of haar in bijvoorbeeld de ledenadministratie is vastgelegd. Meer informatie over AVG is te vinden op: www.protestantsekerk.nl/kerkbeheer/privacy/

## Fraude in de kerk oftewel: zijn de (financiële) afspraken bekend?

Op een zondagmiddag in augustus 2023 kregen verschillende gemeenteleden een mailtje van dominee Giel Schormans (Protestantse Gemeente Voorburg) met een verzoek om geld over te maken voor een bedankje aan vrijwilligers. In werkelijkheid

was het mailtje niet afkomstig van de predikant, maar verstuurd door criminelen met een nagenoeg identiek mailadres, maar ze hadden hotmail.com vervangen voor outlook.com'.

Dit misbruik van gegevens kan zomaar iedereen overkomen, zeker bij ambtsdragers, die met een deel van hun contactgegevens openbaar te vinden zijn. Dit valt nauwelijks aan de voorkant te voorkomen en met de komst van AI zal dit allemaal professioneler en nog echter worden. Criminelen versturen tienduizenden van dit soort mails tegelijk, soms in een paar seconden tijd. Hun 'verdienmodel' is erop gericht dat een paar ontvangers niet naar de afzender kijken en tot betalen overgaan. In een moment van onoplettendheid is dat zo gebeurd.

Toch kun je dit soort situaties tot een minimum beperken door: 1) altijd het daadwerkelijke mailadres te controleren (dus niet alleen de naam van de mailer), 2) zo min mogelijk openbare gegevens op websites te plaatsen, maar vooral door 3) te werken met heldere afspraken over wie er verzoeken om geld kunnen doen en wie deze vervolgens mag goedkeuren en tot betalen kan overgaan. Naarmate er minder bij de kerkenraad bekend is over hoe de financiële afspraken verlopen, des te makkelijker is het voor een crimineel om iemand 'tot betalen' te krijgen. Maar juist als deze vreemde verzoekjes opvallen, omdat ze afwijken van de afspraken, dan zal de afzender nadenken en eventueel navraag gaan doen. Dan komt de fraude snel aan het licht. Dit is een onschuldige vorm, maar er zijn voldoende verhalen bekend over spookfacturen van duizenden euro's naar bankrekeningen van criminelen. Zoals gezegd: dit zal aan de voorkant moeilijk te voorkomen zijn, maar aan de achterkant zijn ze vooral te ontmaskeren door heldere afspraken en open onderlinge communicatie. En bij twijfel geldt ook hier: niet oversteken!

Goed om te weten, dat het ook als kerk mogelijk is om je te laten verzekeren voor de schade als gevolg van datalekken, cyberaanvallen of andere cyberrisks, kijk voor deze mogelijkheden bij onze verzekeringspartner Marsh Mercer: www.kerkrentmeester.nl/home/vkb-verzekeringen/verzekeringsoplossingen/cyberrisks/