POPIA HANDLEIDING VIR DIE NGK GEMEENTE PROTEAHOOGTE

WET OP BESKERMING VAN PERSOONLIKE INLIGTING
Wet no. 4 van 2013

NG GEMEENTE
Proteahoogte
Waar God ons ontmoet en verander vir ander

Tel: 021 982 1041

kkantoor@proteahoogte.co.za |
www.proteahoogte.co.za

Volg ons op Facebook @proteahoogte of
@proteaJeug

Waagmoed | Egtheid | Relevansie | Diversiteit | Afhanklikheid | Gasvryheid

Hoof Inligtingsbeampte

Marili van Tonder
Skriba/ Registerhouer/ Ontvangs

Adjunk inligtingsbeampte

Wanda Gildenhuys
Saakgelastigde/ Finansies

INHOUDSOPGAWE

Voorwaarde 8: Deelname deur “datasubjek”1

1. Wetlike aspekte
2. NGK Proteahoogte Proses

Algemene Bepalings

Uitkontraktering

INLEIDING

1. Doel van die Wet

Tot die bevordering van die beskerming van persoonlike inligting wat deur openbare en privaatliggame geprosesseer word. Dit beteken dat:

- sekere voorwaardes daargestel word ten einde minimum vereistes vir die prosessering van persoonlike inligting te vestig;
- om voorsiening te maak vir instelling van ’n Inligtingsreguleerder om sekere bevoegdhede uit te oefen en om sekere pligte en werksaamhede ingevolge hierdie Wet en die Wet op die Bevordering van Toegang tot Inligting, Wet 2, 2000, te verrig;
- om voorsiening te maak vir die uitreiking van gedragkodes;
- om voorsiening te maak vir die regte van persone met betrekking tot ongeoorloofde elektroniese kommunikasie en geoutomatiseerde besluitneming;
- om die vloei van persoonlike inligting oor die grense van die Republiek te reguleer en
- om voorsiening te maak vir aangeleenthede wat daarmee in verband staan.

Met erkenning dat:

- Artikel 14 van die Grondwet van die Republiek van Suid-Afrika, 1996, voorsiening maak dat elke persoon die reg op privaatheid het;
- die reg op privaatheid ook die reg op die beskerming teen onregmatige insameling, behoud (berging), verspreiding en gebruik van persoonlike inligting behels en
- die Staat die regte in die Handves van Menseregte moet eerbiedig, beskerm, bevorder en verwesentlik.

En gedagtig daaraan dat:

- in ooreenstemming met die grondwetlike waardes van demokrasie en openheid, die noodsaaklikheid vir ekonomiese en sosiale vooruitgang, binne die raamwerk van die inligtingsamelewing, vereis dat onnodige struikelblokke ten opsigte van die vrye vloei van inligting, met inbegrip van persoonlike inligting, verwyder word.

Ten einde:

- die prosessering van persoonlike inligting deur openbare en privaat liggame te reguleer, in harmonie met internasionale standaarde, op ’n wyse wat gevolg gee aan die reg op privaatheid onderhewig aan regverdigbare beperkings wat daarop gemik is om ander regte en belangrike belange te beskerm.

2. Oorsig van die Wet

Hierdie wet is in November 2013 onderteken en gedeeltes het in werking getree in April 2014. In Desember 2016 is die Inligtingsreguleerder aangestel. Die res van die regulasies het op 1 Julie 2020 in werking getree en organisasies (soos bv gemeentes/sinode) moet nou teen 30 Junie 2021 aan alle wetlike vereistes voldoen.

In die omgangstaal word verwys na die wet as POPIA en ons sal deurgaans die afkorting gebruik.

2.1 Wie moet voldoen aan POPIA?

POPIA is van toepassing op enige instansie, maatskappy of organisasie wat op een of ander wyse persoonlike inligting prosesseer. Die Wet geld dus vir openbare liggame (bv Binnelandse Sake, SAID) en private instansies (bv finansiële instellings; gesondheidsorg instansies, besighede, direkte bemarkers, asook kerke).

Die Wet is dus van toepassing op gemeentes, ringe, sinodale en ander kerklike instansies wat op een of ander wyse persoonlike inligting hanteer. Gemeentes wat bv ’n kleuterskool of ouetehuis bedryf, moet ook daarvan bewus wees dat die persoonlike inligting van daardie mense en personeel ook onder POPIA val. Onthou ook dat enige inligting wat ’n gemeente van minderjarige kinders berg, die toestemming van die ouers vooraf verg.

2.2 Wat beteken die prosessering van data/inligting?

Die prosessering van inligting word baie wyd deur die Wet gedefinieer. In terme van POPIA beteken prosessering van inligting enige aksie of aktiwiteit (meganies, outomaties of elektronies) wat die volgende insluit, maar nie daartoe beperk is nie: versameling, ontvangs, opname, organisering, berging, opdatering, herwinning verspreiding, samesmelting, vernietiging en uitwissing van data.

Die beskerming van persoonlike inligting is nou meer as ooit noodsaaklik omdat die ontwikkeling van die elektronika die risiko nog groter maak dat dit misbruik kan word en mense se privaatheid geskend kan word.

2.3 Kan kerke steeds data insamel en prosesseer?

Die Wet verbied niemand om enige persoonlike inligting in te samel en daarmee te handel nie. POPIA skryf net die regmatige handelinge voor om persone te beskerm. Die Wet help om data op die korrekte wyse te prosesseer sonder om vervolging te vrees.

Daarom moet die voldoening aan die vereistes van die Wet nie as las beskou word nie, maar werk dit mee om jouself, ander persone en die kerk te beskerm.

2.4 Wat word beskou as persoonlike inligting?

Uit die onderstaande lys van tipes persoonlike inligting is dit duidelik dat kerklike kantore oor baie persoonlike inligting van lidmate beskik en derhalwe moet daar met sorg daarmee omgegaan word. Hierdie lys dui op die mees algemene inligting waaroor kerkkantore beskik, maar is nie volledig nie.

- Identiteitsnommer/paspoortnommer
- Geboortedatum/ouderdom
- Telefoonnommers
- E-posadresse
- Fisiese adres
- Geslag, ras en etniese oorspring
- Foto's, stemopnames, video-opnames (ook CCTV), biometriese data
- Huwelikstatus en familieverwantskappe
- Kriminele rekord
- Private korrespondensie
- Godsdienstige en filosofiese oortuigings en politieke opinies
- Indiensnemingsrekords en vergoedingsinligting
- Finansiële inligting
- Opvoedkundige inligting
- Fisiese en psigiese gesondheidsinligting, mediese geskiedenis, bloedgroep en seksualiteit
- Lidmaatskap van verenigings en organisasies

Nota: Neem asseblief kennis dat hierdie inligting net van lewendige persone versamel, geberg en gebruik moet word. Inligting wat van persone geberg word wat oorlede is, moet vernietig word (vergelyk voorwaarde 7).

2.5 Hoe kan daar aan POPIA se vereistes voldoen word?

Elke gemeente of kerklike instansie moet aan die volgende aandag gee:

- Die gemeente moet 'n bewusmakingsprogram saamstel en volg.
- 'n POPIA handleiding moet opgestel word.
- 'n Inligtingsbeampte moet aangestel word om toe te sien dat daar aan die eise van die Wet voldoen word.
- Lidmate moet toestemming aan die kerk- of sinodale kantoor verleen om persoonlike data die prosesseer.

2.6 Wat gebeur as daar nie voldoen word aan die wet nie?

Die Wet bepaal ook dat daar ’n maksimum boete van tot en met R 10 miljoen opgelê kan word indien ’n verantwoordelike party nie uitvoering gee aan die bepalings van die Wet nie. Datasubjekte het die reg om ’n regsaksies teen die verantwoordelike party in te stel en dit sou selfs moontlik wees dat, onder sekere omstandighede die Inligtingsbeampte gevangenisskap opgelê kan word.

2.7 Voorwaardes vir voldoening aan die wet?

Verder voorsien die Wet agt (8) voorwaardes waaraan voldoen moet word om persoonlike inligting wettig in te samel, te verwerk, te berg en te gebruik.

Hierdie voorwaardes sal in die volgende hoofstukke bespreek word:
1. Verantwoordingspligtigheid (accountibility)
2. Beperkte prosessering (processing limitation)
3. Oogmerkspesfikasie (purpose spesific)
4. Beperkte verdere prosessering (further processing limitation)
5. Inligtingsgehalte (information quality)
6. Openheid (openness)
7. Veiligheidsvoorsorgmaatreëls (security safeguards)
8. Deelname deur “datasubjek”1

1”datasubjek”- die persoon op wie persoonlike inligting betrekking het

VOORWAARDE 1: VERANTWOORDINGSPLIGTIGHEID

1. Aanstelling van inligtingsbeampte

Marili van Tonder is aangestel as die inligtings beampte vir NGK Proteahoogte en is ingevolge die wet by die toepaslike reguleerder geregistreer. Wanda Gildenhuys is adjunkbeampte en sal in die afwesigheid van Marili haar take oorneem.

2. Die verantwoordelikhede van die Inligtingsbeampte

Dit sluit die volgende in:

- Aanmoediging tot voldoening, deur die instansie, aan die voorwaardes vir die regmatige prosessering van persoonlike inligting.
- Die hantering van versoeke wat ooreenkomstig hierdie Wet aan die liggaam gerig word.
- Om met die Reguleerder saam te werk in verband met ondersoeke wat ooreenstem met Hoofstuk 6 met betrekking tot die instansie gedoen word.
- Om andersins, voldoening deur die instansie aan die bepalings van hierdie Wet te verseker.
- Soos wat voorgeskryf mag word.

Die Inligtingsbeampte ook aan die volgende bykomende vereistes voldoen (Regulasie in Staatskoerant van 14 Desember 2018):

- ’n voldoeningsraamwerk ontwikkel, implementeer, monitor en onderhou.
- ’n persoonlike inligtingsimpakassessering gedoen word om te verseker dat voldoende maatreëls en standaarde bestaan ten einde te voldoen aan die voorwaardes vir die wettige verwerking van persoonlike inligting.
- ’n Handleiding ontwikkel, gemonitor, onderhou en beskikbaar gestel word soos in artikel 11 en 51 van die wet op die Bevordering van Toegang tot Inligting, 2000 (Wet no. 2 van 2000) voorskryf.
- interne maatreëls ontwikkel word saam met voldoende stelsels om versoeke om inligting of toegang te verwerk.
- interne bewustheidsessies oor die bepaling van die Wet, regulasies ingevolge die Wet uitgevaardig, gedragskode of inligting van die Reguleerder verkry, gehou word.

3. Bewusmaking

Bewusmaking en opleiding moet verskaf word aan personeel, gemeenteleiers en groepleiers. Die inligtings beampte, in samewerking met DVK, sal die verantwoordelikheid neem vir hierdie taak.

VOORWAARDE 2: BEPERKTE PROSESSERING

1. Wetlike aspekte

Persoonlike inligting moet

- Regmatig en
- Op ’n redelike wyse wat nie op die privaatheid van die datasubjek inbreuk maak nie, geprosesseer word.

Persoonlike inligting kan slegs geprosesseer word indien:

- ’n bevoegde persoon daartoe toestem.
- direk van die datasubjek ingesamel is.
- in die geval van minderjarige kinders, ’n bevoegde persoon (ouer/voog).
- noodsaaklik is vir die uitvoering van ’n handeling.
- die regmatige belang van die datasubjek beskerm.

Die verantwoordelike party dra die bewyslas vir die datasubjek se toestemming.

2. NGK PH proses

2.1 Verkryging van inligting

Bestaande lidmate van Proteahoogte Gemeente (hierna verwys as PHG) het ‘n Google vorm dmv die gemeente se whatsapp groepe, gekry. Op die vorm is daar opsies om magtiging te gee om huidige inligting wat reeds op die Winkerk stelsel, asook skriftelik in die registerboeke is, te mag berg of ‘n versoek om inligting te vernietig (Bylae 14 of 15). Die toepaslike vorm word dan aan lidmate gestuu. Nadat die vorm voltooi en teruggestuur is aan die kerkkantoor, word dit geliaseer in ‘n POPI leêr.

2.2 Gebruik van inliging

Verder moet ook toestemming verkry word dat hierdie inligting van lidmate gebruik mag word.

Persoonlike inligting word soos volg benut:

- Volle name, nooiensvanne, vanne, ID nommers, geboortedatums, lidmaatstatusse word gebruik om nuwe lidmate se attestate (lidmaatskappe) van hul vorige gemeentes af aan te vra.
- E-pos adresse en selfoonnommers word gebruik om gemeenteskakels aan te stuur aangaande bemarking vir markte, gholfdag en ander gemeente geleenthede (sien Bylae 2 vir lys van alle kerklike aktiwiteite) aan te stuur.

- Die aanlyndienste word per whatsapp uitgestuur tydens die covid tydperk en ook op PHG se “Facebook” bladsy gelaai om gevolg te word.
- Die weeklikse aankondigings word per epos uitgestuur.
- Lidmate se bankbesonderhede word op PHG se Debietordervorm (sien Bylae 3) ingevul, op ons Multidata program gestoor deur Wanda, in ‘n finansiële leêr geliaseer en in die kluis gestoor.

2.3 Toestemming namens minderjariges

Ouers/voogde moet toestemming gee dat minderjariges se inligting versamel, geberg en gebruik mag word. Op die “Nuwe Intrekkersvorm” (sien Bylae 4) sal daar magtiging van nuwe lidmate gevra word om hul minderjarige kinders se inligting te versamel en te berg op ons Winkerk stelsel, asook skriftelik in ons doopregister. Daar is ook ‘n “Ouer toestemming” vorm in plek (sien Bylae 5) wat bestaande minderjarige kategese se ouers kan invul, asook ‘n Doopregistrasievorm (Sien Bylae 6) vir nuwe dopelinge wat ouers kan invul om magtiging te gee om bestaande inligting en nuwe inligting (dopelinge) te versamel en te berg op PHG se Winkerk stel en skriftelik in die doopregister.

2.4. Nuwe lidmate

Proteahoogte Gemeente (hierna verwys as PHG) se “Nuwe Intrekkersvorm” is opdateer om aan die POPIA vereistes te voldoen (sien Bylae 4). Nuwe lidmate moet nou magtiging verleen om hul inligting te kan versamel en berg. Die “Nuwe Intrekkersvorm” is op die webtuiste en in die kerk se voorportaal beskikbaar om ingevul te word. Hul inligting word in die gemeenteregisters aangeteken en op Winkerk stelsel ingesleutel. Net die Hoof inligtings beampte het toegang tot die wagwoord. Daarna word hul attestate (lidmaatskappe) van hul vorige gemeentes af aangevra en sodra dit per epos ontvang is, word die betrokke lidmate in kennis gestel en inligting word op Winkerk aangeteken. Skriftelike vorms en attestate (lidmaatskappe) word in jaar-spesifieke leêrs geliaseer vir 5 jaar en in die kluis gestoor voordat dit na die Kerkargief toe gestuur word.

2.5. Wysiging van inligting

Lidmate moet ook ingelig word van die wyse waarop hulle,

a. Inligting gewysig kan word
   i. ‘n Wysigingsvorm (Sien Bylae 7) sal by die kerkkantoor beskikbaar wees waarop lidmate se inligting gewysig kan word.
   ii. Die wysigingsvorm kan ook per epos aan ‘n lidmaat gestuur word indien die persoon navraag by die kerkkantoor doen.

b. Kerkkantoor versoek om nie meer inligting te ontvang deur
   i. Skriftelik kennis te gee deur ‘n spesifieke vorm (Sien Bylae 8) in te vul met betrekking tot beswaar teen inligting wat ingesamel en geberg word.

ii) Die vorm kan ook per epos aan die lidmaat gestuur word, waar die lidmaat die uitteken opsie **(opt-out funksie)** kan kies en terugstuur aan die kerkkantoor.

2.6. Opdatering van inligting

Inligting/data van lidmate word jaarliks opdateer op die Winkerk stelsel, tensy ‘n lidmaat self die kerkkantoor in kennis stel dat hul inligting verander het. ‘n Wysigingsvorm (Sien Bylae 7) word ingevul en die nuwe/ opgedateerde inligting word dadelik deur die Inligtingsbeampte op die gemeente se Winkerk stelsel opdateer.

VOORWAARDE 3: OOGMERKSPESIFIKASIE

1. Wetlike aspekte

Persoonlike inligting moet:

- Vir ’n bepaalde, uitdruklike omskrewe en regmatige oogmerk wat verband hou met die werksaamhede of aktiwiteite van die gemeente ingesamel word.

Alhoewel artikel 28 van die Wet dit verbied om ’n datasubjek se geloof- en filosofiese oortuigings, in te samel, laat artikel 26 wel ruimte vir kerke om dit te doen.

Magtiging met betrekking tot datasubjek se geloof- of filosofiese oortuiginge

Artikel 28

(1) Die verbod op die prosessering van persoonlike inligting met betrekking tot ’n datasubjek se geloof- of filosofiese oortuiginge, soos in artikel 26 bedoel, is nie van toepassing nie indien die prosessering uitgevoer word deur:

(a) geestelike of geloofsverenigings, of onafhanklike afdelings van daardie verenigings indien
(i) die inligting betrekking het op datasubjekte wat aan daardie verenigings behoort; of
(ii) dit noodsaaklik is om hul oogmerke en beginsels te bereik

(b) instellings gegrond op geloof- of filosofiese beginsels ten opsigte van hul lede of werknemers of ander persone wat aan die instelling behoort, indien dit noodsaaklik is vir die bereiking van hul oogmerke en beginsels

2. NGK PH proses

2.1 Inligting benodig van lidmate

Die volgende inligting word van lidmate benodig:

- Persoonlike inligting: volle name, van, geboortedatum en ID nommer
- Adresbesonderhede: woon- en posadres
- Kontakbesonderhede: telefoon, en selfoonnommers; epos adresse
- Ander inligting: geslag, beroep
- Finansiële inligting: bankbesonderhede

2.2 Bywerk van inligting

Indien gemeentelidmate nuwe inligting aan die kerkkantoor wil deurgee of huidige data wil verander of verwyder/ skrap, kan ‘n spesifieke vorm (sien Bylae 7 en 8) daarvoor aangevra word, ingevul en teruggestuur word, waarná die reggestelling op die Winkerk stelsel gemaak sal word.

VOORWAARDE 4: BEPERKTE VERDERE PROSESSERING

1. Wetlike aspekte

Inligting mag aan sekere groepe in die gemeente verskaf word onder seker voorwaardes.

1.1. Kerkkantoorpersoneel

Administratiewe en finansiële personeel van die gemeente behoort toegang tot lidmate se inligting te verkry en te kan prosesseer.

1.2. Predikante

Dit is noodsaaklik dat predikante die minimum data van lidmate tot hulle beskikking het om hulle ampswerk te kan verrig.

1.3. Kerkraadslede

Kerkraadslede het ook beperkte inligting nodig in die uitvoering van hulle pligte.

4. Bedieninge

Vir Groepleiers, Jeugwerkers en kategese personeel is dit ook noodsaaklik dat hulle oor bepaalde inligting moet beskik om hul werk te verrig. Met die inligting van kinders moet daar baie versigtig te werk gegaan word. Die Wet vereis dat waar minderjarige kinders se inligting geprosesseer word, die ouers/voogde se toestemming nodig is.

2. NGK PH proses

Inligting deur verskillende individue/groepe in die kerk word soos volg hanteer:

2.1. Administratiewe doeleindes

Inligting wat van lidmate versamel word, is:

- Lidmaat se naam, van (en nooiensvan), geboortedatum
- Datum waarop die lidmaat oorgeplaas is na NGK Proteahoogte toe
- Lidmaat se vorige gemeente van waar attestaat/lidmaatskap oorgeplaas is
- Epos adresse en selfoonnommers vir kommunikasie doeleindes bv. whatsapp groepies om belangrike informasie/ skakels aan te stuur ivm eredienste, kategese, markte, basaar, gholfdag en ander belangrike gemeente geleenthede.

2.2 Personeel

- Die hoof inligtingsbeampte het alleenlik toegang tot lidmate se inligting/ data om dit te versamel, verander en te berg op die gemeente se Winkerk stelsel. Die hoof inligtingsbeampte is ook al een wat, met die lidmaat se toestemming (Sien Bylaes 7 en 8), inligting mag verwyder of wysig op die Winkerk stelsel.

- Die finansiële beampte het toegang tot finansiële inligting, soos lidmate se bank besonderhede wat op die opgedateerde Debietordervorm (Sien Bylae 3) ingevul word vir maandelikse aftrekorders. Toestemming word oor hiervoor gegee op die Debietordervorm.

- Die Koster het toegang tot lidmate se inligting wat gebruik word vir begrafnisfunksies (Sien Bylae 9), troufunksies (Sien Bylae 10), algemene funksies (Sien Bylae 11) en nis kontrakte (Sien Bylae 12), soos naam, van, epos adresse en selfoonnommers en ID nommers vir nis kontrakte.

- Die maatskaplike werker is op kontrakbasis en het toegang tot lidmate se inligting, soos naam, van, selfoonnommer, epos adres en woonadres, om sodoende beradingsafsprake na te kom. Die lidmaat kontak die maatskaplike werker direk om ‘n afspraak te maak OF die kerkkantoor hanteer die lidmaat se navraag. Die lidmaat se besonderhede word dan per epos deurgegee aan die maatskaplike werker om op te volg. Die betrokke lidmaat moet hiervoor toestemming gee. (Sien Bylae 13)

Alle personeel moet ‘n ondernemingsvorm (Sien Bylae 14) invul waar hul onderneem om geen inligting aan enige ongemagtigde persoon te verskaf nie, asook om nie die inligting onregmatig te gebruik nie. Die vorm is by die hoof inligtingsbeampte in die kerkkantoor. Personeel moet ten alle tye vertroulikheid handhaaf ten opsigte van die prosessering van persoonlike data/inligting.

2.3 Kerklike Kommunikasie

Inligting van lidmate word deur die kerkkantoor gebruik vir kommunikasie doeleindes soos vir die uitstuur van nuusbriewe en aankondigings per epos, verjaarsdae, whatsapp groepies, sms’e en ander kommunikasie met lidmate.

Die volgende inligting word gebruik vir bogenoemde kommunikasie,

a) Selfoonnommers
b) Epos adresse

2.3. Leraars

Inligting aan leraars word in harde kopie of elektronies beskikbaar gemaak. Die predikante ontvang die kopie by die hoof inligtingsbeampte by die kerkkantoor en teken daarvoor om ontvangs te erken. Die leraars moet ‘n ondernemingsvorm (Sien Bylae 14) teken waar hul onderneem om geen inligting aan enige ongemagtigde persoon te verskaf nie, asook om nie die inligting onregmatig te gebruik nie. Die volgende inligting word per epos aan die betrokke leraar gestuur:

- Indien ‘n paartjie by die kerkkantoor navraag doen oor hul troufunksie, word hul epos adresse, selfoonnommers, troudatum en plek waar bevestiging gaan plaasvind per epos aan die betrokke leraar gestuur.

2.4. Inligting tot beskikking van sekere ampte

- **Kerkraads lede**

Inligting aan kerksraadlede/ groepsleiers word in harde kopie of elektronies beskikbaar gemaak aan hulle. Hulle ontvang die kopie by die hoof inligtingsbeampte by die kerkkantoor en teken ‘n ondernemingsvorm daarvoor om ontvangs te erken en te onderneem om geen inligting aan enige ongemagtigde persoon te verskaf nie, asook om nie die inligting onregmatig te gebruik nie.

Inligting tot beskikking van kerkraadslede:

- Naam, van, nooiensvan
- Eposadresse
- Selfoonnommers
- ID nommers

- **Bedieninge**

PHG se bedieninge is:

- Dare 2 Care
- Gholfdag komitee
- Kommunikasie
- Musiek
- Basaar komitee

Inligting aan bedieninge word in harde kopie of elektronies beskikbaar gemaak aan hulle. Hulle ontvang die kopie by die hoof inligtingsbeampte by die kerkkantoor en teken ‘n ondernemingsvorm daarvoor om ontvangs te erken en onderneem om geen inligting aan enige ongemagtigde persoon te verskaf nie, asook om nie die inligting onregmatig te gebruik nie

Inligting tot beskikking van bedieninge:

- Naam, van
- Eposadresse
- Selfoonnommers

- **Jeug en Kategese**

Die opgedateerde intrekkersvorm (Sien Bylae 4) het ‘n opsie waar ouers magtiging gee aan die kerkkantoor om hul minderjarige kinders se inligting te prosesseer en te berg. Kategese personeel/groepleiers sal ook ontvangs erken vir alle persoonlike inligting wat hulle van die kerkkantoor ontvang en teken ‘n ondernemingsvorm om geen inligting aan enige ongemagtigde persoon te verskaf nie, asook om nie die inligting onregmatig te gebruik nie.

VOORWAARDE 5: INLIGTINGSGEHALTE

1. Wetlike aspekte

Die inligtingsbeampte moet redelikerwys stappe doen ten einde te verseker dat persoonlike inligting volledig, akkuraat is, nie misleidend is nie.

Inligting moet gereeld opgedateer word. Daar moet riglyne geskep word in terme van die siklusse waarin die inligting bygewerk moet word. Daar moet ook bepaal word watter inligting byna nooit verander nie (bv naam, van geboortedatum) en ander inligting wat meermale kan verander (adres, kontakbesonderhede ens).

2. NGK PH proses

2.1 Opdatering van inligting

- Die opdatering van lidmate inligting word jaarliks gedoen. 'n Wysigingsvorm (Sien Bylae 7) is by die kerkkantoor beskikbaar waarop lidmate se inligting gewysig/ verander kan word.
- Die wysigingsvorm kan ook per epos aan 'n lidmaat gestuur word indien die persoon 'n navraag doen deur die kerkkantoor te skakel.
- Die opgedateerde inligting word dan op PHG se Winkerk stelsel ingevoer en ou data/ inligting word afgehaal

2.2 Inligting oudit

'n Oudit van lidmate se inligting word jaarliks gedoen om te bepaal hoe volledig en relevant (op datum) die inligting is. Kontakinligting word nagegaan vir korrektheid. Daar word 'n epos aan die lidmate gestuur dmv. PHG se Mailchimp gemeente eposlys, met 'n aangehegte wysigingsvorm (Sien Bylae 7) waarop veranderinge aangebring kan word, en teruggestuur aan die hoof inligtingsbeampte by die kerkkantoor. Die inligting word dan reggemaak op PHG se Winkerk stelsel.

In die PHG oudit word bepaal:

a. Watter inligting byna nooit verander nie bv persoonlike besonderhede:
   i) ID nommer/ geboortedatum
   ii) Volle name en van (mans)

b. Watter inligting per geleentheid verander:
   i) Nooiensvan (dames)
   ii) Kontakbesonderhede bv. telefoon- en selfoonnommers, eposadresse
   iii) Woon- of posadresse

iv) Huwelikstatusse
v) Lidmaatstatusse (Doop- of belydende lidmate)
vi) Bankbesonderhede van lidmate vir debietorders

c. Watter inligting gereeld nagegaan moet word wat dikwels verander:
i) Kontakbesonderhede soos telefoon- en selfoonnommers
ii) Bankbesonderhede van lidmate (Indien meer as een bankrekening)

VOORWAARDE 6: OPENHEID

1. Wetlike aspekte

Die Wet vereis dat die datasubjek in kennis gestel word wanneer en hoe inligting ingesamel word.

Die verantwoordelike party (gemeente) moet sorg dra vir die volgende:

- Die datasubjek (lidmaat) moet bewus wees van die feit dat sy/haar inligting ingesamel word.
- Wie die inligting insamel (dus die naam en adres van die gemeente).
- Doel waarvoor die inligting ingesamel word.
- Hoe die inligting aangewend gaan word.

2. NGK PH proses

2.1. Openheid

NGK Proteahoogte is ‘n gemeente wat in openheid glo en om aan die wet te voldoen is die volgende in plek gestel:

- Skriftelike aankondiging om gemeente in te lig van die POPI wet 4 van 2013
- ‘n Google vorm (sien bylae 1) waarop lidmate ‘n keuse uitoefen om of toestemming te gee vir hulle huidige data om gestoor te word of om vernietig te word.
- Lys van kerklike aktiwiteite (Sien Bylae 2)
- Debietordervorm is aangepas (Sien Bylae 3)
- Nuwe intrekkersvorm is aangepas (Sien Bylae 4)
- Doopregistrasievorm is aangepas (Sien Bylae 5)
- Opgedateerde Begrafnisvorm (Sien Bylae 6)
- Opgedateerde Trou funksievorm (Sien Bylae 7)
- Opgedateerde Algemene funksievorm (Sien Bylae 8)
- Opgedateerde Niskontrakte (Sien Bylae 9)
- ‘n Ondernemingsvorm (Sien Bylae 10)
- ’n Lys van rekenaartoerusting wat gebruik word om persoonlike inligting op te stoor en te verwerk (Sien Bylae 11)
- ‘n Vorm vir “Ouer toestemming” vir minderjarige kategese (Sien Bylae 12)
- ‘n Wysigingsvorm vir lidmate se inligting (Sien Bylae 13)
- ‘n Vorm vir die beswaar teen verwerking van persoonlike inligting (Sien Bylae 14)
- Toestemmingsvorm van lidmate vir die verwerking van persoonlike inligting vir die doel van direkte bemarking (Sien Bylae 15)

‘n Afskrif van die wet, ‘n Prosedure Handleiding en Beleid oor die hantering van inligting by PH is ten alle tye by Ontvangs en op die webtuiste beskikbaar vir enige lidmaat wat dit wil raadpleeg.

VOORWAARDE 7: VEILIGHEIDSVOORSORGMAATREëLS

1. Wetlike aspekte

Aldus reg 19 is die Kerkraad verantwoordelik vir die veiligheidsmaatreëls om die integriteit en vertroulikheid van persoonlike inligting te waarborg.

(1) die Kerkraad is verantwoordelik vir die integriteit en vertroulikheid van die persoonlike inligting in sy besit of onder sy beheer deur die gebruik van toepaslike, billike tegniese en organisatoriese maatreëls om te voorkom dat daar:

(a) verlies van, skade aan of ongemagtigde vernietiging van persoonlike inligting is; en
(b) onwettige toegang is tot of vir verwerking van persoonlike inligting.

(2) Om uitvoering te gee aan subartikel (1), moet die Kerkraad billike maatreëls in plek stel om:

(a) alle redelike voorsienbare interne en eksterne risiko's vir persoonlike inligting in sy besit of onder sy beheer te identifiseer;
(b) toepaslike veiligheidsmaatreëls teen die geïdentifiseerde risiko's in te stel en te handhaaf;
(c) gereeld te verifieer dat die veiligheidsmaatreëls effektief toegepas word; en
(d) toesien dat die veiligheidsmaatreëls voortdurend opgedateer word in reaksie op nuwe risiko's of tekorte aan voorheen geïmplementeerde veiligheidsmaatreëls.

(3) Die Kerkraad moet die algemeen aanvaarde sekuriteitspraktyke en -prosedures wat gewoonlik van toepassing is of wat in terme van spesifieke bedryfs- of professionele reëls en regulasies vereis word in ag neem.

Inligting van datasubjekte word nie langer as die oorspronklike oogmerk daarvan nie (artikel 14 (1) en (2)), geberg.

Die Wet bepaal egter dat dit wel gebêre mag word in sekere gevalle:

o Historiese, statistiese en navorsings doeleindes, en
o Finansiële inligting

2. NGK PH proses

Gemeente leiers (DVK as verteenwoordiger) sien toe die volgende vier aspekte in plek is:

2.1 Berging van data

Persoonlike inligting word hoofsaaklik op die volgende wyses geberg:

a) Papier weergawes van inligting:

Wanneer daar papier weergawes/ harde kopieë van persoonlike inligting gehou word soos bv. Nuwe Intrekkersvorms, attestate, doop- en lidmaatregisters, dooplyste, belydenis kategeselyste, wykslyste, Sondagskoolklaslyste, Bybelstudiegroeplyste, basaarlyste, marklyste, word dit geliaseer en in die instapkluis weggesluit. Slegs die hoof inligtingsbeampte en Saakgelastigde het sleutels vir toegang tot die kluis.

b) Elektroniese weergawes op e-stelsels:

PHG voer persoonlike data in op stelsels soos Winkerk Online, Mailchimp en Bulk SMS. Die invoer van inligting word slegs op die hoof inligtingsbeampte se skootrekenaar gedoen en sy alleenlik het ‘n wagwoord daarvoor. Mailchimp word deur ons kommunikasie persoon behartig en ‘n ondernemingsvorm word geteken om ontvangs te erken vir alle persoonlike inligting wat hy van die kerkkantoor ontvang en teken ‘n ondernemingsvorm om geen inligting aan enige ongemagtigde persoon te verskaf nie, asook om nie die inligting onregmatig te gebruik nie.

c) Elektroniese dokumente:

Dokumente met persoonlike inligting word versprei in Microsoft Word, Excel formaat en ook as PDF lêers. Die nodige voorsorg moet getref word om hierdie dokumente met ’n wagwoord te beveilig om ongemagtige toegang en lees daarvan te voorkom.

d) E-posadresse:

E-posadresse word veilig op PHG se Winkerk rekenaarstelsel geberg. Slegs die hoof Inligtingsbeampte het toegang tot die wagwoord.

e) Webwerf:

PHG se webwerf verskaf amptenare en bedieningsrade se telefoon- en selfoonnommers, asook eposadresse. Skriftelike toestemming moet verkry word om die inligting te kan publiseer (Sien Bylae 15).

f) Sosiale media:

Toestemming vir die plaas van selfoonnommers, eposadresse en foto’s op Facebook, Twitter en Instagram moet verkry word van die persone wie se inligting of foto’s gebruik word vir die bemarking van kerklike geleente soos bv. die gholfdag, markte, “drive thru” en advertensies oor eredienste. (Sien Bylae 19)

g) Selfone:

Ons gemeente skep dikwels WhatsApp groepe op selfone vir groepskommunikasie. Daar sal skriftelike toestemming verkry moet word dat die persoonlike inligting (selfoonnommers) op ’n toestel geberg mag word en dat dit sigbaar sal wees vir ander groepslede (Sien Bylae 16). Die lidmaat kan die whatsapp groep verlaat deur die “Exit group” opsie te neem.

h) Elektroniese Kommunikasie:

PHG stuur nuusbriewe/ weeklikse aankondigings per e-pos aan gemeentelede. Daar moet skriftelike toestemming van die lidmaat verkry word om sulke kommunikasie te ontvang. ‘n Toestemmingsvorm, om ‘n lidmaat se eposadres te mag gebruik om elektroniese kommunikasie van die kerkkantoor te ontvang, sal per epos aan die lidmaat gestuur word (Sien Bylae 17) Die kommunikasie eposse sal’n “opt-out” opsie hê waar die lidmaat kan onttrek.

2.2 Beveiliging

Inligting word as volg beveilig:

a) **Fisiese sekuriteit:**

Ten opsigte van die fisiese beveiliging van die gebou waar lidmate en amptenare se persoonlike inligting in papier- en elektroniese formaat geberg word, is die volgende in plek:

- Kluis: ’n instapkluis wat groot genoeg is om doop- en lidmaatregisters, leêrs met gemeentelede se inligting/ attestate en ook rekenaartoerusting/ Koster en hoof inligtingsbeampte se skootrekenaars in te berg. Slegs die hoof inligtingsbeampte en Saakgelastigde het toegang tot die instapkluis.

- Diefwering en veiligheidshekke: voor alle vensters en sykantdeure wat na buite oopmaak. Asook voor die ontvangstoonbank. Daar is ook ‘n middeldeur met ‘n veiligheidshek wat gesluit word.

- Alarmstelsel: PHG se alarmstelsel is gekoppel aan ’n reaksie-eenheid.

- Van-terrein beveiliging:
    - ‘n Betroubare diensverskaffer, “Back up Buddy” , word gebruik om inligting van die perseel te stoor.

b) **Elektroniese sekuriteit:**

Ten opsigte van die elektroniese sekuriteit is daar drie belangrike sake nl. Rugsteun, wagwoorde en enkripsie.

• Rugsteun:

o Rugsteun van data op die rekenaarstelsels word daagliks gemaak.
o PHG se rugsteun word deur “Back up Buddy” gedoen. Hierdie eksterne rugsteun is op ’n veilige plek op “Back up Buddy” se “Wolk”.
o Die data word op die “Wolk” geberg sodat dit beveilig is met die nodige sterk wagwoorde wat “Back up Buddy” het. Hulle het alleenlik toegang tot die “Wolk” en PHG kan hul kontak indien enige inligting benodig word.

• Wagwoorde:

o Sterk wagwoorde word gebruik.
o Salestronics word gebruik om die verskillende wagwoorde van databasisse, webwerwe en stelsels op te stel en te bestuur.

• Enkripsie: Die volgende is in plek:

o Antivirusprogram nl. Kapersky
o Kapersky word gebruik om dokumente en eposse te beskerm teen ongemagtigde toegang.

2.3 Data retensie

Die Riglyne vir Bewaring soos deur die Argief van Kaap Kerk wat jaarliks gepubliseer word, word nagevolg. Dit behels:

- Dokumente wat permanent bewaar moet word
  i) Registers
  ii) Agendas en Notules
  iii) Konsistorieboeke
  iv) Afkondigingsboeke
  v) Gemeenteblaaie
  vi) Almanak
  vii) Korrespondensie

- Dokumente wat vir 15 jaar bewaar moet word
  i) Finansiële dokumente (boeke) soos die Kasboek, Grootboek en Joernaal

- Dokumente wat vir 5 jaar bewaar moet word
  i) Geloofsbriewe
  ii) Doopseels
  iii) Lidmaatsertifikate
  iv) Finansiële dokumente ouer as 5 jaar
  v) Basaar-, dankoffer-, en ander kollektelyste

vi) Maandelikse finansiële state
vii) Belastingopgawes

2.4 Vernietiging van data

Vernietiging van dokumente mag slegs plaasvind met die toestemming van die Bestuurder: Argief. Dit is egter die Inligtingsbeampte se verantwoordelikheid om toe te sien dat die volgende vernietig word:

- Oorbodige duplikaat dokumente
- Duplikaatuitdrukke wat as werkskopieë gebruik is
- Lyste met inligting wat nie meer benodig word nie

Vernietiging sal soos volg met sorg geskied:

a) Elektroniese data (rekenaars, dataskywe en geheue stokkies)

- Ou rugsteundata word vernietig, sodat net die nuutste rugsteun beskikbaar is.
- PHG vernietig elektroniese kopieë van inligting wat saamgestel is vir ’n ander doel, maar waarvan die oorspronklike inligting reeds in ons databasisse vasgevang is
- PHG vernietig ou hardeskywe wat nie gebruik word nie.
- Ons maak gebruik van digitale sanitasie om ou rekenaartoerusting skoon te maak. Die uitvee van die geheue is onvoldoende omdat dit gewoonlik net die pad na die rekords uitvee. Die fisiese vernietiging van ou toerusting word ook soms aanbeveel.

b) Harde kopieë (papier rekords)

- Geen dokumente mag vernietig word sonder die goedkeuring van die Argief nie. Goedkeuring moet skriftelik verkry word. Eers word ‘n inventaris opgestel van al die materiaal wat vernietig kan word. Dit word aan die Kerkraad voorgelê vir goedkeuring en daarna aan die Argief as tweede kontrole om seker te maak dat belangrike dokumente nie in die slag bly nie. Eers nadag die Argief toestemming verleen het, mag dié materiaal vernietig word.

- PHG vernietiging harde kopieë vop die volgende manier:
  i) Die harde kopieë word baie fyn opgeskeur word
  ii) Dokumente ouer as 5 jaar word geboks en na die Kerkargief gestuur om vernietig te word.

2.5 Diefstal van inligting

Indien ’n rekenaar en/of hardeskyf gesteel word, sal dit onmiddellik by die SAPD aangemeld word. Die SAPD Saaknommer vir verwysing dat data onregmatig bekom is deur diefstal, sal bewaar word.

VOORWAARDE 8: DEELNAME DEUR DATASUBJEK

1. Wetlike aspekte

Die datasubjek (lidmaat) het die reg om:

1. toegang te hê tot persoonlike inligting wat oor hom/haar gehou word en mag vra om toegang te kry tot eie persoonlike inligting.
2. te versoek dat regstellings of skrapping gemaak word op eie persoonlike inligting en kan ook versoek dat rekords van persoonlike inligting vernietig word.
3. beswaar te maak teen die verwerking van persoonlike inligting.

Lidmate kan ook met inagneming van die Wet op die Bevordering van Toegang tot Inligting (Wet 2 van 2000) PAIA (Promotion of Access to Information Act. Act 2 of 2000) aansoek doen om met die betaling van ’n voorgeskrewe fooi toegang te kry tot inligting.

Ten opsigte van Wet 4 is die volgende vorms beskikbaar op die webblad van die NG Kerk:

• Beswaar teen verwerking van persoonlike inligting (Vorm 1)
• Versoek om regstelling of skrapping van persoonlike inligting of vernietiging of skrapping van rekord van persoonlike inligting (Vorm 2)
• Aansoek om die toestemming van ’n datasubjek vir die verwerking van persoonlike inligting vir die doel van direkte bemarking (Vorm 4)
Nota: Neem kennis dat hierdie “persoonlike inligting” van lidmate wat geberg word, is die beskerming van hierdie inligting nie van toepassing op individue wat meer as twintig [20] jaar oorlede is nie.

2. NGK PH proses

- ‘n Skakel na ‘n Afskrif van die Prosedure Handleiding en Beleid oor die hantering van inligting by NGK Proteahoogte is op die webtuiste (www.proteahoogte.co.za) beskikbaar vir enige lidmaat wat dit wil raadpleeg.
- Die verskeie vorms kan ook van die webblad afgelaai word.
- Die skakels om op Kaapkerk en Kerkargief se web tuistes te gaan: www.kaapkerk.co.za of www.kerkargief.co.za

ALGEMENE BEPALINGS

Regsadvies

Artikel 86 van die Wet bepaal dat kommunikasie tussen ’n kliënt en ’n professionele regsadviseur (sogenaamde “geprivilegeerde inligting”) uitgesluit is van die bepalings van die Wet en lees as volg:

“Kommunikasie tussen regsadviseur en kliënt vrygestel
86. (1) Die bevoegdhede van deursoeking en beslaglegging wat opgedra is deur ’n lasbrief wat kragtens artikel 82 uitgereik is, moet, behoudens die bepalings van hierdie artikel, nie ten opsigte van:

(a) enige kommunikasie tussen ’n professionele regsadviseur en sy of haar kliënt in verband met die verleniging van regsadvies aan die kliënt met betrekking tot sy of haar verpligtinge, aanspreeklikhede of regte; of

(b) enige kommunikasie tussen ’n professionele regsadviseur en sy of haar kliënt, of tussen sodanige adviseur of sy of haar kliënt en ’n ander persoon, in verband met of afwagting van verrigtinge kragtens of voortvloeiend uit hierdie Wet, met inbegrip van verrigtinge voor ’n hof, en vir die oogmerke van sodanige verrigtinge, uitgeoefen word nie.

(2) Subartikel (1) is ook van toepassing op:

(a) ’n afskrif of ander rekord van enige sodanige kommunikasie as wat aldaar vermeld word; en

(b) ’n dokument of artikel ingesluit of na verwys in enige sodanige kommunikasie indien die kommunikasie gedoen is in verband met die verlenging van enige advies of, na gelang van die geval, in verband met of in afwagting van en vir die oogmerke van enige verrigtinge as wat aldaar vermeld word”.

UITKONTRAKTERING

’n Gemeente sou ook kan met ’n onafhanklike operateur ’n kontrak sluit om as agent op te tree ingevolge die Wet.

’n Operateur word omskryf as “’n persoon wat ingevolge ’n kontrak of mandaat persoonlike inligting vir ’n verantwoordelike party (gemeente) prosesseer sonder om onder die direkte gesag van daardie party te wees”. Die kontraktuur is dus nie ’n werknemer nie, maar ’n derde party wat namens die Gemeente die take soos omskryf in POPIA uitvoer.

Die relevante artikels in die Wet is Artikels 20 en 21:

“Inligting geprosesseer deur operateur of persoon wat kragtens magtiging optree
20. ’n Operateur of iemand wat persoonlike inligting namens ’n verantwoordelike party of ’n operateur prosesseer, moet-

(a) sodanige inligting slegs met die kennis of magtiging van die verantwoordelike party prosesseer; en

(b) persoonlike inligting wat tot hul wete kom as vertroulik hanteer en moet dit nie bekend maak nie, tensy dit regtens of in die loop van die behoorlike uitoefening van hul pligte vereis word.

Veiligheidsvoorsorgmaatreëls aangaande inligting deur operateur geprosesseer:

21. (1) ’n Verantwoordelike party moet, ingevolge ’n skriftelike kontrak tussen die verantwoordelike party en die operateur, verseker dat ’n operateur wat persoonlike inligting vir die verantwoordelike party prosesseer veiligheidsvoorsorgmaatreëls, in artikel 19 bedoel, instel en onderhou.

(2) Die operateur moet die verantwoordelike party onmiddellik in kennis stel indien daar redelike gronde is om te vermoed dat ’n ongemagtigde persoon toegang tot die persoonlike inligting van ’n datasubjek verkry het of die persoonlike inligting verkry het”.

Die gemeente sal in haar skriftelike kontrak met die operateur moet toesien dat dit onder andere die volgende bepalings bevat:

- sien toe dat aan die Wet voldoen word en spesifiek Art. 19, dat die veiligheidsvoorsorgmaatreëls getref word;
- onmiddellik die verantwoordelike party inlig indien enige vereistes verbreek is;
- beskerm vertroulike inligting;
- nie persoonlike inligting prosesseer sonder die magtiging of toestemming van die verantwoordelike party nie; en

• toelaat van monitering en ouditering deur die verantwoordelike party om nakoming van die Wet deurgaans te verseker.
• ’n vrywaring van die operateur vereis indien diensvoorwaardes sou verbreek.