POPIA-HANDLEIDING

Hierdie dokument bevat die handleiding van

NG Witbank-Klipfontein Basileia Gemeente

met verwysing na die toepassing van die 8 voorwaardes soos vervat in die wet op die beskerming van persoonlike inligting, Wet no 4 van 2013.

Die POPI-wet handleiding vir kerke

Alles wat kerke moet weet en doen.

(Wet nommer 4 van 2013)

Versuim om te voldoen aan die vereistes van die POPI-wet kan ernstige gevolge hê. Alhoewel mens nie van die wetlike aspekte van die Wet kan en moet wegskram nie, moet die POPI-wet gesien word as 'n geleentheid om inligting beter te identifiseer, te benut en te bestuur om sodoende prosesse in die gemeente te verbeter.

Die wet moet allermins nie iets wees om te vrees of voor bang te wees nie. Gemeentes moet net weet waaroor die wet gaan en wat van hulle verwag word.

INHOUDSOPGAWE

Wet op Beskerming van Persoonlike inligting, No 4, 2013

Inleiding tot die Wet

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 (inligtingsbrief en boodskap is op ons Whatsapp groepe uitgestuur – 30 Junie 2021
- 'n POPIA handleiding moet opgestel word (voltooi 05 Julie 2021)
- 'n Inligtingsbeampte moet aangestel word om toe te sien dat daar aan die eise van die Wet voldoen word (Aangestel & geregistreer – 04 Junie 2021)
- Lidmate moet toestemming aan die kerk- of sinodale kantoor verleen om persoonlike data te prosesseer (toestemmingsbrief en aanbly op whatsapp groepe asook veranderde Nuwe lidmatevorm)

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" ("datasubjek"- die persoon op wie persoonlike inligting betrekking het)

VOORWAARDE 1: VERANTWOORDINGSPLIGTIGHEID

1. Aanstelling van die POPIA-Inligtingsbeampte

1.1 POPIA INLIGTINGSBEAMPTE

Elke gemeente of kerklike instansie moet 'n inligtingsbeampte aanstel soos uiteengesit in die Wet, artikel 55.

Die verantwoordelikhede van so 'n Inligtingsbeampte 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

Verder bepaal artikel 55 (2) dat die Inligtingsbeampte slegs hulle werksaamhede ingevolge hierdie Wet mag opneem nadat die verantwoordelike party hulle by die Reguleerder geregistreer het.

Naas die Wet (artikel 55) moet 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

Die Kerkraad/kerkkantoor moet:

1. 'n Inligtingsbeampte vir die gemeente aanwys
    a. Hierdie inligtingsbeampte:
        i. Is waarskynlik die kerkkantoor personeellid wat gemoeid is met al die data en inligting wat in 'n Kerkkantoor ingesamel, geberg en gebruik word
        ii. het nie spesifieke kwalifikasies en/of opleiding nodig nie
        iii. moet hom/haar gewis van die bepalings van die Wet soos uiteengesit in hierdie handleiding

Die Kerkraad moet die Wet (POPIA) beskikbaar stel aan die inligtingsbeampte. Sien https://www.kerkargief.co.za/inligtingswet/#popia

2. Die Inligtingsbeampte moet in oorleg met die Kerkraad 'n Inligtingsbeleid saamstel.

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Inligtingsbeampte is aangewys en Adjunkinligtingsbeampte is in kennis gestel	04/06/2021	
• Inligtingsbeampte aanwys en registreer by die Reguleerder	04/06/2021	
• Inligtingsbeampte het hom/haarself vergewis van die inhoud van Wet 4 van 2013	04/06/2021	
• Inligtingsbeleid vir die gemeente is saamgestel	In wording	
• Die nodige POPIA skakels vir verdere inligting en klagtes is op die gemeente se webblad aangebring	NVT	
• Die kerkkantoorpersoneel en kerkraad het bewusmaking opleiding ondergaan	**?**	

In terme van die wet op die beskerming van persoonlike inligting, Wet nr 4 van 2013, word die volgende persoon aangestel as die Inligtingsbeampte van die bovermelde instansie.

Naam van Instansie	NG Witbank-Klipfontein Basileia Gemeente	
Registrasienommer		
Tipe Instansie	Openbare Liggaam	Privaatliggaam
Straatadres	70 Hans Strydom Straat Klipfontein Witbank (Emalahleni)	
Posadres	Posbus 12047 Leraatsfontein 1038	
Telefoonnommer	013 697 4449	
Faksnommer		
e-Posadres	klip2@ngklipfontein.co.za	
Selfoonnommer		

Afdeling A Inligtingsbeampte	
Volle name van die Inligtingsbeampte	Martelize Bouwer
Aanstelling / Rol	Skriba / Admin
Posadres	Posbus 12047 Leraatsfontein 1038
Straatadres	70 Hans Strydom Straat Klipfontein Witbank (Emalahleni)

Selfoonnommer	
Landlynnommer	013 697 4449
Direkte e-posadres	klip2@ngklipfontein.co.za
Algemene e-Posadres	
	Ek gee hiermee toestemming dat ek deur die Reguleerder, die aanvraer of datasubjek by bogenoemde kontakinligting gekontak mag word, of deur my aangewese adjunk-inligtingsbeampte (s) wie se inligting hieronder verstrek word.

Afdeling B Adjunk-Inligtingsbeampte			
Persoonlike inligting van aangestelde Adjunk-Inligtingsbeampte(s)	Naam en Van	Naam en Van	Naam en Van
	Adri Lenting		
	Direkte landlyn	Direkte landlyn	Direkte landlyn
	013 697 4449		
	Selfoonnommer	Selfoonnommer	Selfoonnommer
	e-Posadres	e-Posadres	e-Posadres
	admin@ngklipfontein.co.za		
Posadres	Posbus 12047 Leraatsfontein 1038		
Straatadres	70 Hans Strydom Straat Klipfontein Witbank (Emalahleni)		
Faksnommer			
Algemene e-Posadres			

Ek verklaar dat die inligting hierin waar, korrek en akkuraat is.

GETEKEN en GEDATEER te ___Witbank _____ op _____04 Junie_____2021

_____M Bouwer_____

INLIGTINGSBEAMPTE

SERTIFIKAAT van Registrasie ontvang per epos op 04 Junie 2021 vanaf Itirele
itirele@justice.gov.za

1.2 POPIA PROSEDURE HANDLEIDING

Elke Inligtingsbeampte moet 'n Prosedure Handleiding saamstel wat aan die vereistes van die Wet voldoen. Die Kerkraad moet hierdie handleiding goedkeur. Hierdie handleiding het ten doel om die gemeente se beleid ten opsigte van die verskering van privaatheid te bepaal.

Die handleiding moet die volgende bevat:

a. Data insameling (Punt 2 hieronder)
    1. Tipe data
    2. Doel waarvoor die data ingesamel word
    3. Toestemming van datasubjek (lidmate)
    4. Berging van data (Minimalistiese berging)
    5. Deursigtigheid
    6. Toegang tot data
b. Data gebruik en beperkings (Punt 3 hieronder)
c. Data berging (Punt 4 hieronder) (**c, d, e en f word ook in Voorwaarde 7 bespreek**)
d. Data beveiliging (Punt 5 hieronder)
e. Data retensie (Punt 6 hieronder)
f. Data vernietiging (Punt 7 hieronder)
g. Personeel bewustheidsopleiding (Punt 8 hieronder)
h. Publisering van die handleiding (Punt 9 hieronder)

Wat betref die data van die datasubjek (lidmaat) moet die volgende aandag kry:

- **Insameling**: die verskillende tipe inligting wat versamel gaan word, moet omskryf word
- **Gebruik en beperkings**: hoe die data gebruik gaan word, moet omskryf word. Verder moet dit duidelik gestel word waarvoor die data aangewend gaan word vir die interne funksionering van die gemeente. Dit moet ook duidelik gestel word dat geen data aan ongemagtigde persone beskikbaar gestel sal word nie
- **Berging**: 'n omskrywing van hoe en waar die data geberg gaan word
- **Beveiliging**: omskryf hoe die data beveilig sal word in terme van fisiese en elektroniese sekuriteit
- **Retensie**: hoe lank word die data geberg
- **Vernietiging**: volledige beskrywing hoe die onbenutte en/of verouderde data vernietig gaan word

Die Kerkraad/kerkkantoor moet:

1. Die Inligtingsbeampte moet in oorleg met die Kerkraad ŉ Inligtingsbeleid en prosedure handleiding vir gebruik in die gemeente saamstel.
2. Die Inligtingsbeleid en prosedure handleiding moet die volgende bevat:
    a. Welke persoon verantwoordelik is vir die insameling, bewaring en gebruik van lidmate se inligting
    a. Watter inligting word deur die Kerkkantoor versamel, geberg en gebruik, bv lidmaat inligting ens
    b. Hantering van inligting wat bepaal:
        i. Op welke wyse die instemming van lidmate verkry word om die inligting te versamel, te berg en te gebruik
        ii. Hoe toestemming van ouers verkry word wanneer inligting van minderjariges hanteer word
        iii. Wysigings van inligting verkry vanaf die lidmate (datasubjekte)
    c. Metodes wat gebruik word om inligting te berg:
        i. Skriftelike data
        ii. Elektroniese data
    d. Metodes om inligting te beveilig:
        i. Skriftelike data bv bewaar in kluis
        ii. Elektroniese data: wagwoorde ens
    e. Tydperk vir bewaring van inligting
        i. Watter inligting word hoe lank geberg
        ii. Hoe inligting bv geargiveer word
    f. Vernietiging van inligting
        i. Skriftelike data bv versnippering
        ii. Elektroniese data wat uitgewis word
    g. Gebruik van inligting
        i. Waarvoor word watter inligting gebruik
        ii. Doelspesifiek data vir sekere ampte bv wat kry leraar, kerkraadslede ens
3. Sodra die Inligtingsbeampte die inligtingsbeleid en prosedure handleiding gefinaliseer het, moet alle personeellede wat op een of ander wyse van die data gebruik maak, opleiding ontvang om hulle bewus te maak van die vereistes van die Wet en hoe daar voortaan met data gewerk gaan word.

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Inligtingsbeleid is saamgestel		Besig daarmee
• Interne opleiding is verskaf oor hoe om met inligting om te gaan, na aanleiding van die Inligtingsbeleid		

2. Data - Insameling

Die volgende riglyne word toegepas met die proses van insameling van data:

1. Tipe data wat ingesamel word

Persoonlike Inligting

Die volgende persoonlike inligting kan versamel word, hoewel nie alles van elke persoon noodwendig versamel gaan word nie.

- Van
- Nooiensvan
- Volle name
- Noemnaam
- Geboortedatum
- Voorletters
- Titel
- ID Nommer
- Geslag
- Woonadres
- Posadres
- Landlynnommer
- Selfoon
- Werktelefoon
- Faks
- e-Posadres
- Beroep
- Werkgewer
- Foto van individu of gesin
- Huwelikstatus
- Huweliksdatum
- Gesinshoof of gesinslid
- Rol in die gesin

Kerklike Inligting

Die volgende kerklike inligting kan versamel word, hoewel nie alles van elke persoon noodwendig versamel gaan word nie.

- Lidmaatstatus
- Bewysstatus
- Aansluitmetode
- Datum Ontvang
- Vorige Gemeente
- Wyk / Bediening
- Predikantswyk
- Verskillende groepe waaraan die persoon behoort asook die rol in die groep.

- Aansluit- en uittreedatums m.b.t. groepe.
- Meelewings
- Gawes
- Passies
- Doopdatums, ouers se vanne en volle name, predikant wat die doop bedien het
- Belydenisafleggingsdatums en datum toegelaat tot belydenisaflegging asook die predikant voor wie belydenis afgelê is.

Bankbesonderhede

Die volgende bankbesonderhede kan versamel word, hoewel nie alles van elke persoon noodwendig versamel gaan word nie. Die inligting word slegs gebruik indien daar van 'n debietorderstelsel gebruikgemaak word. Waarvan ons NG Witbank- Klipfontein Basileia Gemeente nie gebruik maak nie.

- Takkode
- Rekeningnaam
- Rekeningnommer
- Tipe rekening

Mediese besonderhede

Die volgende mediese besonderhede kan versamel word, hoewel nie alles van elke persoon noodwendig versamel gaan word nie. Die inligting word hoofsaaklik slegs gebruik by kinders se besonderhede, en slegs indien die kind onder toesig van die kerkraad iewers op 'n uitstappie / kamp / uitreik heen geneem sou word.

- Mediesefonds naam
- Mediesefonds nommer
- Hooflid se naam
- Afhanklike kode
- Huisdokter
- Huisdokter telefoonnommer
- Noodkontakpersoon naam
- Noodkontakpersoon telefoonnommer
- Allergieë
- Chroniese Medikasie

2. Doel waarvoor data benodig word

Die doel van die versameling van persoonlike data van lidmate is, omdat die persoon 'n lid van 'n organisasie, by name, **NG Witbank -Klipfontein Basileia Gemeente,** is. Lidmaatskap van 'n kerk is presies dieselfde as om 'n lid van enige ander organisasie te wees. Dit gaan dikwels nodig wees om nuwe meelewings of gawes of mylpale van lidmate by te voeg of te verander, of ou inligting te verwyder. Lidmate se tipe lidmaatskap kan ook verander, of kontakinligting kan verander. Daarom is dit noodsaaklik dat daar 'n proses van instandhouding van data moet wees. Kontak met lidmate is soms op 'n baie gereelde basis nodig en sodanige kontak geskied deur die persoonlike inligting van

lidmate. Artikel 28 van die wet gee spesifiek vir kerke die toestemming om lidmate se inligting te mag versamel en te bewaar.

3. Toestemming van lidmate

[BESKRYF IN HIERDIE AFDELING OP WATTER MANIERE U VOORAF TOESTEMMING VAN LIDMATE VERKRY OM HULLE DATA TE MAG VERWERK.]

Ons gaan ‘n toestemmingsbrief met ons lidmate op die Whatsapp groepe deel en hulle ook herinner om hulle inligting met ons te kommunikeer indien dit verander het en hulle ook daaraan herinner dat indien hulle nie daarmee saamstem nie, dat hulle welkom is om die groep te verlaat. Ons noem ook daarin dat ouers toestemming gee vir die verwerking van hulle kinders se inligting. (Brief ook hierby aangeheg onder Addendums.)

Persoonlike inligting mag slegs op billike en wettige wyse versamel en verwerk word en slegs met toestemming van die betrokke persoon. Vir daardie rede het ons gemeente 'n "**Nuwe lidmatevorm**" wat aan lidmate voorsien word waarop hulle, hulle inligting moet voltooi en dit moet ook deur die lidmaat onderteken word om te bevestig dat hy/sy goedkeuring verleen dat die inligting wat hy/sy voorsien deur die gemeente gestoor mag word. Dit is baie belangrik om daarop te let dat in terme van die wet ouers ook toestemming moet verleen dat die gemeente die data van minderjarige kinders mag stoor. Die Nuwe lidmatevorm maak spesifiek ook daarvoor voorsiening. Die nuwe lidmatevorm maak spesifiek voorsiening vir die lidmaat se handtekening.

Ons moet seker maak dat die lidmaat wel die vorm onderteken het wanneer ons dit in ontvangs neem. ‘n Vorm sonder ‘n handtekening beteken eintlik dat die lidmaat nie sy of haar goedkeuring verleen het nie. Let ook asb. daarop dat waar twee belydende lidmate se inligting op die vorm voorkom, benodig ons die handtekening van beide lidmate. Dit is ook ‘n goeie idee om hierdie nuwe lidmatevorm te stoor. Die vorm kan as ‘n .pdf of .jpg lêer gestoor word en deur middel van Winkerk se “Attachment” funksie na die C:\Winkerk 7 gids op die hardeskyf gekopieer word. **Maak baie seker dat hierdie gids geënkripteer moet wees.**

4. Minimalistiese berging (Beperkte prosessering)

Dit is ook belangrik dat ons nie alles oor 'n lidmaat hoef te versamel en te stoor nie. Ons het net slegs en alleenlik die inligting nodig om ons bediening met die lidmaat te kan verrig. Indien 'n gemeente al die inligting oor 'n lidmaat invoer wat in Winkerk ingevoer kan word oor 'n lidmaat, voldoen dit steeds aan die minimalistiese voorskrif. Die inligting wat Winkerk versamel oor 'n lidmaat is sodanig saamgestel dat elke stukkie inligting wat versamel word, deeglik gemotiveer kan word, waarvoor dit benodig word. (Sien ook die beskrywing van inligting in nommer 1)

5. Deursigtigheid

Ons gemeente se beleid is baie duidelik dat ons geen inligting sal verberg waaroor ons beskik nie, en dat ons geen inligting bewaar wat ons nie bereid is om bekend te maak nie.

[Dit is belangrik dat gemeentes nie een ding moet sê en 'n ander ding doen nie. Moenie voorgee dat u minder inligting oor hulle stoor as wat u werklik doen nie of dat u alles in u vermoë doen om die lidmaat se inligting veilig te bewaar terwyl dit nie gedoen word nie. Lidmate moet op enige stadium kan versoek om die inligting wat u stoor, te mag sien. Sien ook die Infokerk Opmerking by par 6 oor die toegang tot data.]

6. Toegang tot data

[BESKRYF IN HIERDIE AFDELING OP WATTER MANIERE U LIDMATE TOEGANG TOT HULLE EIE DATA KAN VOORSIEN]

Lidmate kan 'n epos rig na klip2@ngklipfontein om hulle data op te dateer. Hulle kan ook na die Kerkkantoor kom en hulle inligting in Winkerk bevestig of 'n "Nuwe lidmate vorm kan ingevul word om hulle data op te dateer. Hulle is te enige tyd welkom om toegang tot hulle eie date te bekom.

Lidmate moet toegang tot hulle data hê (Art 23), en volgens die wet ook die data kan wysig of 'n versoek tot wysiging aanhangig maak (Art 24). Toegang tot die data beteken nie noodwendig dat die lidmaat toegang tot die gemeente se Winkerk program moet kan kry nie. 'n Verslag van alle data van die lidmaat wat die gemeente bewaar, sou voldoende wees.

Indien die lidmaat dus sou reageer op die verslag en versoek dat sekere data gewysig moet word, moet die gemeente die veranderinge aanbring en weer 'n nuwe verslag aan die lidmaat voorsien.

LW: Nie alle versoeke van lidmate tot verandering van data moet net voor die voet uitgevoer word sonder om die wysigings te verifieer nie. 'n Lidmaat sou bv. nie kon versoek dat sy of haar volle name of van gewysig word, sonder dat stawende bewyse van die departement van Binnelandse Sake voorsien word nie.

LW: Alvorens enige versoek tot toegang of wysiging van data uitgevoer mag word , MOET SODANIGE VERSOEK OP 'N VOORGESKREWE VORM GEDOEN WORD EN STAWENDE IDENTIFIKASIE MOET VOORGELê WORD OM TE BEVESTIG DAT DIE AANSOEKER WEL IS WIE HY/SY BEWEER OM TE WEES.

Winkerk Online is juis ontwerp om vir gemeentes die instrument te wees wat daarvoor aangewend kan word. Let asb. daarop dat wanneer lidmate in Winkerk Online veranderinge aan hulle data aanbring, is dit heeltemal in lyn met die POPI wet se voorskrif, maar ons het dit sodanig ontwerp dat die Winkerk gebruiker steeds in beheer van die data is. Alle wysigings wat lidmate in Winkerk Online aanbring, is slegs versoeke tot verandering en moet steeds deur die Winkerk gebruiker in Winkerk goedgekeur word. Die lidmaat kry egter outomaties in Winkerk Online terugvoering van die proses en hoe ver die versoek reeds deur die gemeente geprosesseer is.

3. Data gebruik en beperkings. (Beperkte verdere prosessering.)

(Sien ook Voorwaarde 4 p26 hieronder)

BESKRYF IN HIERDIE AFDELING WATTER PERSONE TANS TOEGANG TOT DIE DATA HET EN WATTER INLIGTING HULLE IN DIE TOEKOMS MAG SIEN.]

Wie kry tans toegang tot die data?

Die volgende persone of instansies binne die gemeente kry tans toegang tot die lidmate se data.

Kerkkantoor personeel

Die administratiewe en finansiële personeel kan toegang tot die data verkry, hoewel die minimalistiese beginsel steeds toegepas moet word.

In die verband is dit baie belangrik dat gemeentes tyd moet begroot om te bepaal wie almal toegang tot Winkerk het, en seker te maak dat slegs amptenare wat werklik toegang tot alle data moet kry, sodanige regte binne in Winkerk moet ontvang, wat hulle toegang tot alle data gee. Om toegang tot alle data te ontvang, beteken nie noodwendig dat so 'n amptenaar enige data moet kan verander nie. Dit is heeltemal moontlik dat 'n Winkerk gebruiker wel alle data kan sien, maar nie wysig nie. Dit is baie belangrik slegs een gebruiker as "meester gebruiker" aangestel moet word. Die meester gebruiker is dan die enigste gebruiker wat ander gebruikers se regte kan verander. Alle ander amptenare se regte kan individueel verstel word onder die "Stelsel opsie" by die afdeling "Gebruikers" om slegs beperkte toegang met beperkte regte aan hulle toe te ken. Ons het ook onlangs 'n funksie bygevoeg waar elke gebruiker wat in Winkerk aanteken, verplig word om 'n skerm te "onderteken" waarin hulle onderneem om die inligting van lidmate te beskerm en nie aan enige ongemagtigde persoon of instansie ooit sal bekend maak nie.

Die "REGTE" van Winkerk gebruikers raak veral belangrik met die gebruik van Winkerk 10]

Predikante

Dit is noodsaaklik dat predikante wel toegang tot die data van alle lidmate moet kan kry om hulle ampsverpligtinge ten volle te kan nakom. Hierdie inligting is meestal; naam & van, telefoon nommer en adres (indien besoek moet word).

Natuurlik moet die minimalistiese beginsel ook hier toegepas word. Predikante en ander amptenare moet net van die minimum inligting voorsien word, en sou die behoefte later verander dat hulle meer inligting nodig kry om hulle werk te kan doen, kan dit op daardie stadium aan hulle beskikbaar gestel word. Maak ook seker dat die volgende inligting met die betrokke amptenaar gekommunikeer word wanneer inligting aan hulle voorsien word.

Kerkraadslede

Dit is natuurlik ook noodsaaklik dat kerkraadslede in die uitvoering van hulle pligte sekere inligting van lidmate moet hê. Hierdie inligting is gewoonlik; naam & van en telefoon nommer.

Maak seker dat hierdie inligting ook tot die minimum beperk word en dat die riglyne soos hierbo vir predikante ook nagekom word. Inligting wat aan kerkraadslede voorsien word, behoort beperk te word, tot die lidmate van hulle bediening. Dit is nie nodig dat 'n kerkraadslid inligting van lidmate in ander bedienings hoef te hê nie, behalwe waar die kerkraadslid verantwoordelik is vir meer as een bediening.

Jeugwerkers en Sondagskoolpersoneel

Dit is verder ook noodsaaklik dat Jeugwerkers en Sondagskoolpersoneel in die uitvoering van hulle pligte sekere inligting van lidmate moet hê. Hierdie inligting is gewoonlik; naam & van en telefoon nommer van die kinders sowel as van die ouers.

Maak seker dat hierdie inligting ook tot die minimum beperk word en dat die riglyne soos hierbo vir predikante ook nagekom word. Dit is verder ook baie belangrik om daarop te let dat die inligting van kinders spesifiek baie beperk word deur die wet en dat daar oor die algemeen baie versigtiger met die inligting van kinders omgegaan moet word. Die wet vereis ook dat, om die inligting van minderjarige kinders te mag berg, die toestemming van die ouers nodig is.

Lidmate

Lidmate kan natuurlik ook beperkte toegang tot inligting van ander lidmate kry. Hierdie inligting is gewoonlik; naam & van en telefoon nommer.

Dit gebeur baie maal dat herdenkings of verjaardae op die gemeente se afkondigings verskyn. Hierdie inligting is dan nie alleen vir die gemeente sigbaar nie, maar ook vir die wyer publiek. Dit is daarom noodsaaklik dat persoonlike inligting van lidmate wat op openbare platforms soos webwerwe, sosiale media of selfs WhatsApp, asook afkondigings voorkom, slegs gepubliseer mag word met die **toestemming van die lidmaat**.

4. Data berging

[BESKRYF IN HIERDIE AFDELING WAAR DATA GEBERG WORD. MAAK SEKER DAT U TEN VOLLE BEWUS IS VAN WAAR DAAR WINKERK PROGRAMME GELAAI IS EN DEUR WIE DIT GEBRUIK WORD. U MOET VERDER BESKRYF WAAR ANDERS OOK INLIGTING VAN LIDMATE GESTOOR WORD.]

1. Elektronies

Winkerk 7 of 10

Kerkkantoor:

Die eerste en belangrikste versamelpunt van inligting van lidmate is Winkerk 7 of Winkerk 10.

Addisionele installasies van Winkerk:

Admin personeel se tuisrekenaars.

Die lisensiërings ooreenkoms van Infokerk met die gemeente, maak voorsiening daarvoor dat Winkerk op meer as een rekenaar gebruik mag word, sonder ekstra kostes.

Hoewel Winkerk 10 heeltemal POPI-aanpasbaar is, is dit steeds net 'n rekenaarprogram wat deur operateurs gebruik word en derhalwe is daar sekere voorskrifte wat nagekom moet word. Gemeentes wat nog Winkerk 7 gebruik, word sterk aangemoedig om so spoedig moontlik oor te gaan na Winkerk 10, sodra dit beskikbaar word. Dit is egter belangrik dat die POPI-inligtingsbeampte van die kerkraad deeglik bewus moet wees op watter rekenaars Winkerk gebruik word, en daar moet voortdurend geëvalueer word of daardie installasies steeds benodig word.

'n Skriba kon moontlik toestemming by die kerkraad gekry het om Winkerk op sy/haar persoonlike rekenaar by die huis te installeer. Dieselfde reëls wat geld vir die beskerming van die data by die kerkkantoor, geld ook inderdaad vir die skriba se persoonlike rekenaar. Sou die skriba bedank by die gemeente, of nie meer die program benodig nie, moet die POPI-inligtingsbeampte toesien dat die program en die data van die skriba se tuisrekenaar verwyder word. Enige van Infokerk se takkantore kan gekontak word, om hiermee behulpsaam te wees. Dit is nie op ons van toepassing nie.

Onthou ook dat alle rugsteun kopieë van die Winkerk data, sowel as enige ander elektroniese dokument wat moontlik inligting van lidmate mag bevat ook verwyder moet word.

Predikante se rekenaars.

Dieselfde beginsels wat geld vir die skriba se tuisrekenaars, geld net so ook vir predikante se tuisrekenaars.

Winkerk Online

Kerkkantoor personeel kan toegang kry tot Winkerk Online.

1. Dit is van uiterste belang dat die POPI-inligtingsbeampte ook moet weet watter amptenare toegang tot Winkerk Online verkry het, sodat hy/sy ook kan verseker dat persone se toegang herroep kan word, indien hulle nie meer die toegang benodig nie.

2. Dit is ook in elk geval goeie praktyk om van tyd tot tyd wagwoorde wel te verander.

Lidmate kan ook as Lidmaatgebruikers toegang kry tot Winkerk Online.

Lidmate kan toegang kry tot hulle eie data in Winkerk Online. Sodra 'n lidmaat oorgeplaas word na 'n ander gemeente, of bedank uit die gemeente sal die lidmaat nie meer in Winkerk Online toegang tot daardie data kan verkry nie. Die argiveringsproses van die lidmaat in Winkerk 7 ontkoppel die lidmaat outomaties van die data in Winkerk Online.

Finkerk 3

Die normale sinchronisasieproses tussen Winkerk en Finkerk skryf ook persoonlike inligting van lidmate soos van, name, geboortedatum, selfoon, e-posadres asook straat- en posadres oor na die Finkerk databasis. Ons maak nie van Finkerk gebruik nie.

Die Finkerk databasis is nog 'n Microsoft Access databasis en sou dmv. Microsoft Access gelees kan word. Ter wille van POPI-aanpasbaarheid, het ons egter 'n wagwoord op die Finkerk databasis geplaas wat slegs aan sommige Infokerk personeellede bekend is. Dit is ongelukkig so dat as 'n gemeente se Finkerk databasis lank gelede geskep is, dit nie met die wagwoord beskerm sal wees nie. Ons wil gemeentes aanmoedig om die hoofkantoor van Infokerk te kontak ten einde vas te stel of u gemeente se Finkerk data met 'n wagwoord beskerm is of nie. Indien dit nie met 'n wagwoord beskerm is nie, sal ons u kan help om die wagwoord daarop aan te bring.

Backup Buddy

Backup Buddy maak weekliks 'n rugsteun van die gemeente se Winkerk- en/of Finkerk data. Hierdie rugsteun kopie word dan opgelaai na Infokerk se "Cloud Server."

Die rugsteun kopieë word in die oplaaiproses met 'n baie sterk wagwoord beskerm alvorens dit die gemeente se rekenaar verlaat. Daar word egter 'n plaaslike kopie van die rugsteun op die gemeente se rekenaar gestoor. Die doel van hierdie plaaslike kopie is vir interne gebruik van die gemeente en die lêer wat gerugsteun is, is nie met 'n wagwoord beskerm nie.

E-Pos programme

Ons gebruik Microsoft Outlook en elke rekenaar het 'n wagwoord voordat daar toegang tot die epos verkry kan word.

Woordverwerkings- en sigbladprogramme

BESKRYF IN HIERDIE AFDELING WATTER WOORDVERWERKINGS- EN SIGBLADPROGRAMME U GEBRUIK.

Ons gebruik Microsoft office pakket en elke rekenaar het 'n wagwoord voordat daar toegang tot die programme verkry kan word.

Gemeentelike webwerwe

BESKRYF IN HIERDIE AFDELING OF U GEMEENTE 'N WEBWERF HET EN INDIEN WEL WATTER INLIGTING DAAR GEDRA WORD.

Ons gemeente het nie op die oomblik 'n webwerf nie.

Selfone

BESKRYF IN HIERDIE AFDELING OF U GEMEENTE INLIGTING VAN LIDMATE OP SELFONE STOOR EN INDIEN WEL OP WATTER SELFONE.

Die kantoor selfoon het al die lidmate se nommers en name op vir die gebruik van die Whatsapp groepe.

2. Harde kopieë

BESKRYF IN HIERDIE AFDELING OF U GEMEENTE HARDE KOPIEë DRUK EN INDIEN WEL, WAAR WORD DIT GEBERG EN AAN WIE EN HOE DIT AAN HULLE VOORSIEN WORD.

Lessenaarlaaie

Indien verslae in lessenaarlaaie geberg word, word dit sterk aanbeveel dat die laaie gesluit behoort te word, sodra die gebruiker van die lessenaar af wegbeweeg.

Liasseerkabinette

Dieselfde beginsel wat vir lessenaarlaaie geld, geld natuurlik ook vir liasseerkabinette. Liasseerkabinette bevat natuurlik 'n groter versameling van inligting en behoort daarom beter beskerm te word.

5. Data beveiliging

1. Elektronies

Stappe in die beveiliging van elektroniese data.

1.1 Fisiese sekuriteit van die kantoor.

BESKRYF IN HIERDIE AFDELING WATTER MEGANISMES U IN PLEK GESTEL HET VIR DIE FISIESE SEKURITEIT VAN DIE PERSEEL.

Ons kantoor beskik oor fisiese sekuriteit soos veiligheidshekke en diefwering. Ons het 'n kamerastelsel, alarmstelsel en instapkluis.

Die begroting van die gemeente sal bepalend wees van die mate van die fisiese sekuriteit wat in die kantoor aangebring kan word. Die mees basiese vorm van sekuriteit is waarskynlik om te verseker dat daar ten minste diefwering en veiligheidshekke aangebring moet word. Indien die begroting dit toelaat

sal sekuriteitskameras en 'n alarmstelsel 'n waardevolle toevoeging tot die fisiese sekuriteit van die kantoor wees.

Dit moet natuurlik by die personeel ingeskerp word dat veiligheidshekke gesluit moet wees en alarmstelsels geaktiveer moet word sodra die kantoor verlaat word. Dit help niks as die kantoor die beste veiligheidsmaatreëls het, maar dit word nie gebruik nie.

'n Volgende stap in die fisiese sekuriteit van die kantoor sou wees, indien die gemeente se begroting dit sou toelaat en dit prakties moontlik is, om 'n groot genoeg kluis te hê waarin alle dokumente met persoonlike inligting van lidmate in geberg kan word asook 'n lêerbediener daarin te stoor.

1.2 Elektroniese sekuriteit.

BESKRYF IN HIERDIE AFDELING IN GROOT DETAIL AL DIE MEGANISMES WAT U IN WERKING GESTEL HET OM ALLE ELEKTRONIESE DATA TE BESKERM. – SIEN GERUS DIE INFOKERK POPI-KURSUS VIR VOLLEDIGE BESONDERHEDE IN DIE VERBAND.]

Ons kantoor maak gebruik van wagwoorde op elke rekenaar voordat daar toegang tot enige program verkry kan word. Winkerk het ook 'n wagwoord.

2. Harde kopieë

Stappe in die beveiliging van harde kopieë.

BESKRYF IN HIERDIE AFDELING WATTER STAPPE U GENEEM HET OM HARDE KOPIEë TE BESKERM. – SIEN GERUS DIE INFOKERK POPI-KURSUS VIR VOLLEDIGE INLIGTING IN DIE VERBAND

Al ons kantoor se harde kopieë is of in die argief of in die kluis gebêre.

6. Data retensie

BESKRYF IN HIERDIE AFDELING HOE LANK DATA BEWAAR WORD. SIEN GERUS DIE INFOKERK POPI-KURSUS VIR VOLLEDIGE BESONDERHEDE IN DIE VERBAND

Data word vir solank as deur die Sinode voorgeskryf gebêre.

7. Data vernietinging

BESKRYF IN HIERDIE AFDELING WATTER MEGANISMES U IN PLEK STEL OM HARDE KOPIEë, ELEKTRONIESE DATA ASOOK OU HARDEWARE TE VERNIETIG. . SIEN GERUS DIE INFOKERK POPI-KURSUS VIR VOLLEDIGE BESONDERHEDE IN DIE VERBAND

Ons data word dienooreenkomstig met die Sinode voorgeskrewe vernietigingsproses vernietig.

8. Personeel bewustheidsopleiding

Personeel bewustheidsopleiding moet deur die POPI-inligtingsbeampte gedoen word. Dit is egter nie iets wat slegs eenmalig gedoen kan word nie, maar moet op 'n gereelde basis aangebied word. Dit is ook nie iets wat net vir nuwe personeel aangebied moet word nie, maar alle bestaande personeel moet weer opgeskerp word in terme van die gemeente se POPI-beleid.

9. Publisering van die handleiding

Hierdie handleiding sal slegs in die Kerkkantoor van NG Witbank-Klipfontein Basileia Gemeente beskikbaar wees as 'n harde kopie.

VOORWAARDE 2: BEPERKTE PROSESSERING

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

Die Kerkraad/kerkkantoor moet:

’n Proses bepaal hoe:

1. Bestaande lidmate se toestemming verkry behoort te word dat hulle inligting, versamel en geberg is.
2. Verder moet toestemming ook verkry word dat hierdie inligting van lidmate gebruik mag word. Voorbeelde van hoe die inligting gebruik kan word, moet verskaf word.
3. Wyse waarop ouer/voogde toestemming gee dat minderjariges se inligting versamel, geberg en gebruik mag word
4. Nuwe lidmate moet ook toestemming verleen dat hulle inligting versamel, geberg en gebruikmag word dmv ons nuwe lidmatevorm
5. Lidmate moet ook ingelig word van die wyse waarop hulle
    a. Inligting gewysig kan word – epos aan klip2@ngklipfontein.co.za te stuur.
    b. Kerkkantoor versoek om nie meer inligting te ontvang deur
        i. Skriftelik kennis te gee
        ii. ’n Uitteken opsie (*opt-out* funksie) of Whatsapp groep/e te verlaat
6. Bepaal hoe dikwels die inligting opgedateer word

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Bestaande lidmate herbevestig dat persoonlike inligting gebruik mag word	30 Junie 2021	
• Nuwe intrekkervorms gewysig sodat toestemming verkry kan word vir insameling en berging	30 Junie 2021	
• Waar inligting van kinders gebruik word moet spesifiek gevra word en vorm moet dit aandui		
• Elektroniese kommunikasie het ’n “opt out” funksie		Kan Whatsapp groep verlaat
• Skriftelike toestemming is ontvang om persoonlike inligting op gemeente se webblad, afkondigings, inligtingsbrosjures, facebook, ens te publiseer	nvt	

VOORWAARDE 3: OOGMERKSPESIFIKASIE

Persoonlike inligting moet:

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

Die handleiding moet die volgende omskryf:

Watter inligting benodig word

Hoe die inligting bygewerk word wat verander

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

Die Kerkraad/kerkkantoor moet die volgende bepaal ten opsigte van:

1. Watter inligting van lidmate ingesamel gaan word soos byvoorbeeld:
    a. Persoonlike inligting bv: volle name, van, geboortedatum en identiteitsnommer
    b. Adresbesonderhede bv: woon- en posadres
    c. Kontakbesonderhede bv: telefoon, en selfoonnommers; epos adresse
    d. Ander inligting bv.: geslag, taalvoorkeur, beroep
    e. Finansiële inligting, bv: bankbesonderhede

2. Bepaling van doeleindes waarvoor die inligting gebruik gaan word

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Maak ’n lys van alle tipes inligting wat ingesamel word. Heg dit aan as ’n byvoegsel tot die handleiding		Sien nr 2 hierbo p 15

VOORWAARDE 4: BEPERKTE VERDERE PROSESSERING

Die Kerkraad moet bepaal watter personeel/lidmate toegang tot watter persoonlike inligting mag verkry.

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

   Dit kan in harde kopie of elektronies beskikbaar gemaak word. Die inligting moet so beskikbaar gestel word, dat die predikante die kopie in ontvangs neem en daarvoor ontvangs erken. Die beste is dat dit genommerde kopie is wat weer later terugbesorg kan word vir vernietiging. Indien dit elektronies beskikbaar gestel word, moet daar verkieslik 'n wagwoord ook gegee word om toegang te verkry.

2. Kerkkantoorpersoneel
   Administratiewe en finansiële personeel van die gemeente behoort toegang tot lidmate se inligting te verkry en te kan prosesseer. Van die personeel kan toegang tot die inligting kry, maar daar moet reëlings getref word wie die inligting kan wysig of verander. Daar moet 'n prosedure geskep word en toestemming gegee word ten opsigte van die personeellid wat die inligting kan wysig. Daar moet dus 'n "hoof" of "meester" gebruiker aangewys word wat ook ander gebruikers van die nodige inligting kan voorsien.

   Personeel moet ook 'n onderneming gee om nie inligting aan enige ongemagtigde persoon te verskaf nie asook om nie die inligting onregmatig te gebruik nie. Personeel moet ten alle tye vertroulikheid handhaaf ten opsigte van die prosessering van persoonlike data / inligting.

3. Kerkraadslede
   Kerkraadslede het ook beperkte inligting nodig in die uitvoering van hulle pligte. Daar moet riglyne gegee word oor die minimum inligting wat hulle benodig en dit moet aan hulle beskikbaar gestel word. Kerkraadslede behoort ook net die inligting te kry in die bedienings waar hulle werk en nie van ander wyke nie.

   Dieselfde reëling moet getref word vir bv., omgeeleiers en hulle groepe of ander belangegroepe se leiers.

   Kerkraadslede/groepleiers moet ontvangs erken vir alle persoonlike inligting wat hulle van die kerkkantoor ontvang vir gemeentelike gebruik.

4. Jeugwerkers en Kategese Skool personeel (Tiener en Kinderbediening)
   Vir Jeugwerkers en kategese personeel is dit ook noodsaaklik dat hulle oor bepaalde inligting moet beskik om hulle werk te verrig.

   ONTHOU: 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.

   Kategese personeel / (Tiener / kinderbedienings) groepleiers moet ontvangs erken vir alle persoonlike inligting wat hulle van die kerkkantoor ontvang.

Die Kerkraad/kerkkantoor moet bepaal wie toegang tot die inligting het:

1. Watter inligting word vir administratiewe doeleindes versamel bv vir lidmaatregisters
2. Inligting wat deur die kantoor gebruik word vir bv Nuusbriewe, afkondigings, bedieningsindelings, verjaarsdae, sms en ander kommunikasie met lidmate
3. Inligting wat aan leraars voorsien moet word
4. Inligting tot beskikking van sekere ampte – bv Lidmate in bediening vir bepaalde bedieningsleier

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Maak ’n lys van alle persone, groepe, komitees, ens wat toegang moet kry tot sekere tipes inligting en dui aan waarvoor dit benodig word. Heg dit aan as ’n byvoegsel tot die handleiding.		Nr 3 p 18

VOORWAARDE 5: INLIGTINGSGEHALTE

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).

Die Kerkraad/kerkkantoor moet bepaal:

1. Hoe die inligting op datum gehou word
2. Gereeld ’n oudit doen om te bepaal hoe volledig en relevant (op datum) die inligting is
3. In die oudit moet bepaal word:
    a. Watter inligting byna nooit verander nie bv persoonlike besonderhede
    b. Watter inligting per geleentheid verander bv nooiensvan, kontakbesonderhede
    c. Watter inligting gereeld nagegaan moet word wat dikwels verander, bv kontakbesonderhede soos telefoonnommers

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Stel ’n proses in plek om ten minste jaarliks kontakinligting na te gaan vir korrektheid.		# lidmate versoek om inligting op te dateer. # Jaarliks Whatsapp gemeente herinner om inligting op te dateer. # Winkerk op datum # Met kursus inskrywings verifieer ons die inligting
• Bepaal watter inligting met watter intervalle opdateer moet word.		Soos ons inligting ontvang sal ons dit opdateer en dan jaarliks herinner.

VOORWAARDE 6: OPENHEID

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

Die Kerkraad/kerkkantoor moet lidmate inlig:

1. Dat hulle inligting versamel, geberg en gebruik word
2. Waarvoor die verskillende “vlakke” van inligting gebruik gaan word

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Soos in voorwaarde twee: Nuwe intrekkervorms gewysig, sodat toestemming verkry kan word vir insameling en berging	Joey nuwe vorm gemaak 30 Junie 2021	

VOORWAARDE 7: VEILIGHEIDSVOORSORGMAATREËLS

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.

Die Kerkraad/kerkkantoor moet toesien dat die volgende vier aspekte in plek is:

1. **Berging van data (Sien ook punt 4 p19 hierbo)**

   Wanneer daar besin word oor die berging van persoonlike inligting moet besluit word watter tipe data versamel word en wie toegang daartoe moet verkry. Dit is bepalend in die wyse waarop data geberg en beskikbaar gemaak word. Die formaat, hetsy elektroniese of papier kopie bepaal ook die berging van die inligting. Persoonlike inligting word hoofsaaklik op die volgende wyses geberg:

   a) Papier weergawes van inligting: Wanneer daar papier weergawes van persoonlike inligting gehou word soos bv in doop en lidmaatregisters, bedieningslyste, Sondagskoolklaslyste, Bybelstudiegroeplyste, basaarlyste, ens moet dit in ’n kluis weggesluit word.
   b) Elektroniese weergawes op e-stelsels: gemeentes wat persoonlike data invoer op stelsels soos Winkerk, Dolos, Finkerk, Winkerk Online, ens moet bepaal op watter toestelle hierdie sagteware

beskikbaar is (bv tafelrekenaars, skootrekenaars, tablette en selfone) en verseker dat die nodige sekuriteit in plek is – nie net fisiese berging nie, maar ook toegang tot die elektroniese data (Sien ook punt 2)

c) Elektroniese dokumente: Dokumente met persoonlike inligting word dikwels versprei in Microsoft Word en Excel formaat en ook as PDF lêers. Die nodige voorsorg moet getref word, sodat hierdie dokumente met 'n wagwoord beveilig is om ongemagtige toegang en lees daarvan te voorkom.
d) E-posadresse: E-posadresse wat op rekenaarstelsels geberg word kan op verskillende maniere geberg word, bv lokaal op die hardeskyf of soos bv Gmail in die wolk. Daar moet toegesien word dat dit beveilig is teen ongemagtigde toegang.
e) Webwerf: Webwerwe verskaf dikwels persoonlike inligting oor amptenare en gemeentelede. Sien toe dat skriftelike toestemming ontvang is om die inligting te publiseer. Wanneer inligting oor kinders geplaas word, is die skriftelike toestemming van beide ouers/voog ook nodig. Verseker ook dat die wagwoorde vir gebruik deur die webmeester beveilig is.
f) Sosiale media: Soos met webwerwe geld dieselfde reëls vir die plaas van persoonlike inligting op Facebook, Twitter en Instagram.
g) Selfone: Gemeentes skep dikwels WhatsApp groepe op selfone vir groepskommunikasie. Daar moet verseker word dat skriftelike toestemming ontvang is dat die persoonlike inligting (selnommers) op 'n toestel geberg mag word en dat dit sigbaar sal wees vir ander groepslede. Die lidmaat moet die opsie hê om die groep te kan verlaat.
h) Elektroniese Kommunikasie: Gemeentes stuur dikwels kennisgewings oor eredienste, gemeentlike aktiwiteite en Nuusbriewe per e-pos aan gemeentelede. Daar moet skriftelike toestemming van die lidmaat wees om sulke kommunikasie te ontvang en die geleentheid moet daar wees om te kan onttrek. Dit is belangrik dat hierdie e-posse dan 'n "opt-out" opsie moet hê waar die lidmaat kan onttrek.

2. Beveiliging (Sien ook punt 5 p 21 hierbo)

Kerkrade moet aandag gee aan die fisiese en elektroniese beveiliging van persoonlike inligting.
Fisiese sekuriteit: Ten opsigte van die fisiese beveiliging van die gebou waar persoonlike inligting in papier en elektroniese formaat geberg word moet verseker word dat die volgende in plek is:

- Kluis: Verkieslik 'n instapkluis wat groot genoeg is om registers en ook rekenaartoerusting in te berg.
- Diefwering: voor alle vensters en deure wat na buite oopmaak.
- Alarmstelsel: verkieslik 'n alarmstelsel wat gekoppel is aan 'n reaksie-eenheid.
- Sekuriteitskameras: waar moontlik 'n kamera-stelsel, sodat toegang tot die terrein en gebou gemonitor kan word.
- Van-terrein beveiliging: Maak seker dat die volgende in plek is:
    - Rekenaarhardeskywe (ekstern en geheuestokkies) veilig gestoor word.
    - Skootrekenaars beveilig is en bewaar word.

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

- Rugsteun: As 'n sekerheidsmaatreël maak seker dat
    - Rugsteun gereeld gemaak word van data op rekenaarstelsels
    - Bewaar hierdie eksterne rugsteun op 'n veilige plek. Dit is dikwels aan te raai dat dit op 'n ander terrein is.
    - Indien dit op die Wolk geberg word, dat dit beveilig is met die nodige sterk wagwoorde.
- Wagwoorde: Maak seker dat
    - Sterk wagwoorde gebruik word
    - Gereelde verandering van wagwoorde plaasvind
    - 'n Wagwoordbestuurderprogram gebruik word om al die verskillende wagwoorde van databasisse, webwerwe en stelsels bestuur kan word.

- Enkripsie: Maak seker dat die volgende in plek is
    - Antivirusprogramme
    - Enkripsie programme gebruik word waar moontlik om dokumente te beskerm teen ongemagtigde toegang.

3. Data retensie (Sien ook punt 6 p 22 hierbo)

Die Wet vereis dat inligting van datasubjekte nie langer geberg mag word as die oorspronklike oogmerk daarvan nie (artikel 14 (1) en (2)). Die Wet bepaal egter dat dit wel gebêre mag word in sekere gevalle:

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

Raadpleeg hiervoor die Riglyne vir Bewaring soos deur die Argief van jaar tot jaar gepubliseer word. (skakel na Webwerf) Vorm ook in Addendum van lêer asook inventaris vorm

Die Wet bepaal ook dat inligting gehou mag word as dit benodig word vir die funksionering van die organisasie.

4. Vernietiging van data (Sien ook punt 7 p 22 hierbo)

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, ens.

Vernietiging moet met sorg geskied.

- <u>Elektroniese data</u> (rekenaars, dataskywe en geheue stokkies)
    - Hoe rugsteundata moet vernietig word, sodat net die nuutste rugsteun beskikbaar is. Dit is goeie praktyk om weergawes te bestuur (version control).
    - Vernietig elektroniese kopieë van inligting wat saamgestel is vir ’n ander doel, maar waarvan die oorspronklike inligting reeds in databasisse vasgevang is.
    - Vernietig ou hardeskywe wat in onbruik is.
    - 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.
- <u>Harde kopieë</u> (papier rekords)
    - Vermy om onnodige papier-uitdrukke van persoonlike data te maak.
    - Moenie ongebruikte of ou inligtingstukke in die snippermandjie gooi nie.
    - Sien toe dat dit verbrand, versnipper of verpulp word.

5. Diefstal

Indien ’n rekenaar en/of hardeskyf gesteel word, meld onmiddellik aan by SAPD. Bewaar die SAPD Saaknommer vir verwysing dat data onregmatig bekom is deur diefstal

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Papierweergawes van doop- en lidmaatregisters; papierweergawes van persoonlike inligting op databasisse word in ’n kluis gebêre	Reeds gedoen	
• ’n Lys van rekenaartoerusting wat gebruik word om persoonlike inligting op te stoor en te verwerk is gemaak en aangeheg as ’n bylaag tot die handleiding.	Slegs kantoorpersoneel se rekenaartoerusting	
• Wagwoorde bestaan vir elke stuk rekenaartoerusting wat gebruik word.	Ja	
• E-Posadresse is beveilig met ’n wagwoord	Ingangswagwoord vir rekenaar	
• Toestemming is ontvang van elke persoon van wie daar persoonlike inligting op die webwerf gepubliseer is.		
• Die wagwoorde wat deur die webmeester gebruik word, is beveilig	Ja	
• Skriftelike toestemming is van lidmate ontvang om persoonlike inligting op sosiale media te plaas		
• Lidmate moet skriftelik toestemming gee om op WhatsApp groepe gevoeg te word	Ja	
• Ontvangers van boodskappe op sosiale media moet die geleentheid hê om te kan “opt out.”	Ja of whatsapp groep te verlaat	
• Skriftelike toestemming is ontvang van lidmate om Nuusbriewe per e-pos te ontvang. Daar moet ’n “opt out” opsie beskikbaar wees	Ja	

• Kerkkantoor beskik oor:
  ○ Instapkluis
  ○ Klein kluis
	Ja	

• Kerkkantoor beskik oor:
  ○ Diefwering
  ○ Veiligheidshekke
  ○ Alarmstelsel
  ○ Sekuriteitskameras
	Ja	

• Daar is ’n register van eksterne rekenaarhardeskywe, geheuestokkies en kontrole oor waar dit is		
• Daar word op ’n gereelde grondslag rugsteun van databasisse gedoen	Ja	
• Daar word van ’n wagwoordbestuurder gebruik gemaak om wagwoorde te bestuur en te beskerm		
• Daar is antivirusprogramme op alle rekenaars gelaai	Ja	
• Daar word van enkripsie programme gebruik gemaak om persoonlike data te beveilig		
• Daar word jaarliks by die Argief aansoek gedoen om in terme van voorgeskrewe beleid vernietigings te doen	Ja	
• Daar word op ’n jaarlikse basis in terme van die voorgeskrewe beleid dokumente na die Argief gestuur vir veilige bewaring	Nee ons bewaar self ons dokumente	
• Ou rekenaartoerusting word wanneer nodig op korrekte wyse vernietig	Ja	
• Die kerkkantoor beskik oor ’n versnipperaar	Ja	

VOORWAARDE 8: DEELNAME DEUR DATASUBJEK

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. (Kerkargief.co.za – die Vorms is ook as Addendums in die lêer).

- 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.

Die Kerkraad/kerkkantoor moet

Moet toesien dat daar op hul webblad ’n skakel is waar die aansoekvorms of afgelaai kan word en/of ’n skakel na die NG Kerk se bladsy is om dit te doen.

KONTROLELYS		
Aktiwiteit	Datum voltooi	Remedie
• Vorms 1 -3 is beskikbaar op die gemeente se webblad		
• Daar is ’n proses in plek hoe aansoeke hanteer word		

Regsadvies

Artikel 86 van die Wet bepaal dat kommunikasie tussen ŉ kliënt en ŉ 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 ŉ lasbrief wat kragtens artikel 82 uitgereik is, moet, behoudens die bepalings van hierdie artikel, nie ten opsigte van-*

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

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

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

(b) ŉ 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

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

ŉ Operateur word omskryf as "'ŉ persoon wat ingevolge ŉ kontrak of mandaat persoonlike inligting vir ŉ verantwoordelike party (gemeente) prosesseer sonder om onder die direkte gesag van daardie party te wees". Die kontrakteur is dus nie ŉ werknemer nie, maar ŉ 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**. ŉ Operateur of iemand wat persoonlike inligting namens ŉ verantwoordelike party of ŉ 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) ŉ Verantwoordelike party moet, ingevolge ŉ skriftelike kontrak tussen die verantwoordelike party en die operateur, verseker dat ŉ 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 ŉ ongemagtigde persoon toegang tot die persoonlike inligting van ŉ 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.
- ŉ vrywaring van die operateur vereis indien diensvoorwaardes sou verbreek.

Ons gemeente, NG Witbank-Klipfontein Basileia Gemeente maak nie gebruik van Uitkontraktering nie.

_____oOo_____