Nederduitse Gereformeerde Kerk
EEN LIGGAAM EN EEN GEES

POPIA HANDLEIDING

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

PROTECTION OF PERSONAL INFORMATION
Act 4 of 2013

Riglyne aan Sinodale en gemeente kantore om te voldoen aan die vereistes van die Wet

Saamgestel deur:
Dr Andrew Kok
Argivaris van die Ned Gerf Kerk

Dr Dewyk Ungerer
Aktuarius van die Algemene Sinode

Maart 2021

<table>
<tr><td colspan="3">POPIA HANDLEIDING VIR DIE
NG GEMEENTE ______________________ (vul eie gemeente naam in)</td></tr>
<tr><td>Inligtingsreguleerder</td><td>Adv Pansy Tlakula</td><td>JD House
Stiemensstraat 27
Braamfontein
Johannesburg

Posbus 31533
Braamfontein
Johannesburg
2017

inforeg@justice.gov.za</td></tr>
<tr><td>Hoofinligtingsbeampte</td><td>Dr Gustav Claassen</td><td>Posbus 13528
Hatfield
0028

tel 012 342 0092

info@ngkerk.org.za
gensecdrc@ngkerk.org.za</td></tr>
<tr><td>Adjunkinligtingsbeampte</td><td>Dr Andrew Kok</td><td>NG Kerk Argief
Noordwal-wes 1
Stellenbosch

Posbus 34
Stellenbosch
7599

021 882 9923

argief@kaapkerk.co.za</td></tr>
<tr><td>Gemeente Inligtingsbeampte</td><td>Eie besonderhede</td><td>Kontakbesonderhede van gemeente/sinode</td></tr>
</table>

INLEIDING

WET OP BESKERMING VAN PEROONLIKE 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 ŉ 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
- 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 ŉ 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 privaat 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. ŉ 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 ŉ 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 verbeid 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 <u>Hoe kan daar aan POPIA se vereistes voldoen word?</u>

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 <u>Wat gebeur as daar nie voldoen word aan die wet nie?</u>

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 <u>Voorwaardes vir voldoening aan die wet?</u>

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

1.1 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		
• Inligtingsbeampte aanwys en registreer by die Reguleerder		
• Inligtingsbeampte het hom/haarself vergewis van die inhoud van Wet 4 van 2013		
• Inligtingsbeleid vir die gemeente is saamgestel		
• Die nodige POPIA skakels vir verdere inligting en klagtes is op die gemeente se webblad aangebring		
• Die kerkkantoorpersoneel en kerkraad het bewusmakings-opleiding ondergaan		

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
    i. Tipe data
    ii. Doel waarvoor die data ingesamel word
    iii. Toestemming van datasubjek (lidmate)
    iv. Berging van data
    v. Deursigtigheid

        vi. Toegang tot data
b. Data gebruik en beperkings
c. Data berging
d. Data beveiliging
e. Data retensie
f. Data vernietiging
g. Personeel bewustheidsopleiding
h. Publisering van die handleiding

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 ’n 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		
• Interne opleiding is verskaf oor hoe om met inligting om te gaan, na aanleiding van die Inligtingsbeleid		

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 gebruik mag word
5. Lidmate moet ook ingelig word van die wyse waarop hulle
    a. Inligting gewysig kan word
    b. Kerkkantoor versoek om nie meer inligting te ontvang deur
        i. Skriftelik kennis te gee
        ii. ’n Uitteken opsie (*opt-out* funksie)
6. Bepaal hoe dikwels die inligting opgedateer word

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

VOORWAARDE 4: 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 geloofs- en filosofiese oortuigings, in te samel, laat artikel 26 wel ruimte vir kerke om dit te doen

> Magtiging met betrekking tot datasubjek se geloofs- of filosofiese oortuiginge
>
> Artikel 28
> (1) Die verbod op die prosessering van persoonlike inligting met betrekking tot ’n datasubjek se geloofs- 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 geloofs- 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 bv.:**
   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.		

VOORWAARDE 5: 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 ŉ wagwoord ook gegee word om toegang te verkry

2. Kerkkantoorpersoneel
   Administratiewe en finansiële personeel van die gemeenste 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 ŉ prosedure geskep werd en toestemming gegee word ten opsigte van die personeellid wat die inligting kan wysig. Daar moet dus ŉ "hoof" of "meester" gebruiker aangewys word wat ook ander gebruikers van die nodige inligting kan voorsien.

   Personeel moet ook ŉ 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 wyke 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
   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/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, wykindelings, 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 wyk vir bepaalde ouderling/diaken**

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.		

VOORWAARDE 6: 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.		

• Bepaal watter inligting met watter intervalle opdateer moet word.		

VOORWAARDE 7: 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		

HOOFSTUK 8: 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 in 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

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, wykslyste, 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 he 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

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

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)

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

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, ens.

Vernietiging moet met sorg geskied.

- <u>Elektroniese data</u> (rekenaars, dataskywe en geheue stokkies)
    - Hou 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.

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		
• ’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.		
• Wagwoorde bestaan vir elke stuk rekenaartoerusting wat gebruik word.		
• E-Posadresse is beveilig met ’n wagwoord		
• 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		
• 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		
• Ontvangers van boodskappe op sosiale media moet die geleentheid hê om te kan “opt out.”		
• Skriftelike toestemming is ontvang van lidmate om		

Nuusbriewe per e-pos te ontvang. Daar moet ’n “opt out” opsie beskikbaar wees		
• Kerkkantoor beskik oor: o Instapkluis o Klein kluis		
• Kerkkantoor beskik oor: o Diefwering o Veiligheidshekke o Alarmstelsel o Sekuriteitskameras		
• Daar is ’n register van eksterne rekenaarhardeskywe, geheuestokkies en kontrole oor waar dit is		
• Daar word op ’n gereelde grondslag rugsteun van databasisse gedoen		
• Daar word van ’n wagwoordbestuurder gebruik gemaak om wagwoorde te bestuur en te beskerm		
• Daar is antivirusprogramme op alle rekenaars gelaai		
• 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		
• Daar word op ’n jaarlikse basis in terme van die voorgeskrewe beleid dokumente na die Argief gestuur vir veilige bewaring		

• Ou rekenaartoerusting word wanneer nodig op korrekte wyse vernietig		
• Die kerkkantoor beskik oor ’n versnipperaar		

VOORWAARDE 9: 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 in agneming 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.

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		

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.

oOo