Nederduitse Gereformeerde Kerk in Suid-Afrika
ngkadmin@kaapkerk.co.za – https://www.kaapkerkadmin.co.za
Privaatsak X8, Bellville, 7535 – 021 957 7104
PBO 9300 13251

Beleid 21.4
Wet op Beskerming van Persoonlike Inligting

Doel:	Handleiding om die NG Kerk in SA se beleid ten opsigte van die Wet op Beskerming van Persoonlike Inligting (Wet 4 van 2013) aan elke werknemer, taakspan en diensgroep te verduidelik.
Eienaar:	Inligtingsbeampte
Funksionaris verantwoordelik vir hierdie beleid:	Saakgelastigde
Implementeringsdatum:	1 Julie 2021
Hersieningsdatum:	Jaarliks tydens die tweede kwartaal se vergadering van die Sinodale Taakspan vir Finansies en Administrasie
Datum van hierdie weergawe:	1 Julie 2021
Weergawenommer:	21.4

WET OP BESKERMING VAN PERSOONLIKE INLIGTING
WET 4 VAN 2013
(POPIA – Protection of Personal Information Act)

Beleid van die
Nederduitse Gereformeerde Kerk in Suid-Afrika

IDENTIFISERENDE BESONDERHEDE

Die Inligtingsreguleerder

Straatadres:	JD House, Stiemenstraat 27, Braamfontein, Johannesburg, 2001
Posadres:	Posbus 31533, Braamfontein, Johannesburg, 2017
Klagtes e-pos:	complaints.IR@justice.gov.za
Algemene e-posse:	inforeg@justice.gov.za
Webwerf:	https://www.justice.gov.za/inforeg/index.html

Die Hoofinligtingsbeampte van die Nederduitse Gereformeerde Kerk in Suid-Afrika

Hoofinligtingsbeampte:	Die Saakgelastigde, ds CJ Stander
Straatadres:	NG Kerksentrum, De Langestraat 5, Bellville, 7530
Posadres:	Privaatsak X8, Bellville, 7535
Telefoon:	021 957 7104
E-pos:	ngkadmin@kaapkerk.co.za
Webwerf:	https://www.kaapkerkadmin.co.za/ https://www.kerkargief.co.za/

INLEIDING

1. Doel van die Wet

Die doel van Wet 4 van 2013 is die bevordering van die beskerming van persoonlike inligting wat deur openbare en privaatliggame geprosesseer word.

1.1 Dit beteken dat

1.1.1 sekere voorwaardes daargestel word ten einde minimum vereistes vir die prosessering van persoonlike inligting te vestig;

1.1.2 om voorsiening te maak vir die 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 van 2000, te verrig;

1.1.3 om voorsiening te maak vir die uitreiking van gedragkodes;

1.1.4 om voorsiening te maak vir die regte van persone met betrekking tot ongeoorloofde elektroniese kommunikasie en geoutomatiseerde besluitneming;

1.1.5 om die vloei van persoonlike inligting oor die grense van die Republiek te reguleer en

1.1.6 om voorsiening te maak vir aangeleenthede wat daarmee in verband staan.

1.2 Met erkenning dat

1.2.1 Artikel 14 van die Grondwet van die Republiek van Suid-Afrika, 1996, voorsiening maak dat elke persoon die reg op privaatheid het;

1.2.2 die reg op privaatheid ook die reg op die beskerming teen onregmatige insameling, behoud (berging), verspreiding en gebruik van persoonlike inligting behels en

1.2.3 die Staat die regte in die Handves van Menseregte moet eerbiedig, beskerm, bevorder en verwesentlik.

1.3 En gedagtig daaraan dat

1.3.1 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.

1.4 Ten einde

1.4.1 die prosessering van persoonlike inligting deur openbare en privaatliggame 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 se regte en belangrike belange te beskerm.

2. Oorsig van die Wet

Wet 4 van 2013 is in November 2013 onderteken en gedeeltes het in werking getree in April 2014. Die Inligtingsreguleerder is in Desember 2016 aangestel. Die res van die regulasies het op 1 Julie 2020 in werking getree en organisasies (soos die Nederduitse Gereformeerde Kerk in Suid-Afrika) moet vanaf 1 Julie 2021 aan alle wetlike vereistes voldoen.

In die omgangstaal word verwys na die wet as **POPIA** (*Protection of Personal Information Act*). Hierdie handleiding gebruik hierdie afkorting.

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 en private instansies soos kerke.

Die Wet is dus van toepassing op alle diensgroepe en taakspanne van die kerk wat op een of ander wyse persoonlike inligting hanteer.

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 elektroniese tegnologie die risiko nog groter maak dat dit misbruik kan word en mense se privaatheid geskend kan word.

2.3 Kan diensgroepe / taakspanne 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.

Die voldoening aan die vereistes van die Wet moet nie as ’n las beskou word nie. Die Wet werk mee om die werknemer, ander persone en die kerk te beskerm.

2.4 Wat word beskou as persoonlike inligting?

Uit die onderstaande lys van die soort van persoonlike inligting waarmee sinodale kantore werk, is dit duidelik dat daar met groot omsigtigheid daarmee gehandel moet word:

- Identiteitsnommer/paspoortnommer
- Geboortedatum/ouderdom
- Telefoonnommers/Selfoonnommers
- E-posadresse
- Fisiese adresse
- Geslag, ras, taal en kultuur
- Opvoedkundige inligting /Akademiese kwalifikasies
- Huwelikstatus en familieverwantskappe
- Godsdienstige en filosofiese oortuigings
- Werkgeskiedenis en indiensnemingsrekords
- Vergoedingsinligting en ander finansiële inligting
- Fisiese en psigiese gesondheidsinligting, mediese geskiedenis en bloedgroep
- Seksualiteit
- Foto’s, stemopnames en video-opnames (ook CCTV)
- Private korrespondensie
- Lidmaatskap van verenigings en organisasies
- Psigometriese toetsuitslae
- Kriminele rekord
- Sterfdatum

2.5 Hoe kan daar aan POPIA se vereistes voldoen word?

2.5.1 Elke diensgroep en taakspan moet aan die volgende aandag gee:

2.5.1.1 Die diensgroep moet ’n bewusmakingsprogram saamstel en volg;
2.5.1.2 Hierdie POPIA-handleiding moet gereeld met alle personeel behandel word;
2.5.1.3 Elke diensgroep moet ’n adjunkinligtingsbeampte aanstel wat toesien dat daar aan die eise van die Wet voldoen word en
2.5.1.4 Datasubjekte moet toestemming aan die sinodale kantoor verleen om persoonlike data die prosesseer.

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

Die Wet bepaal dat ’n maksimum boete van tot en met R10 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

Die Wet voorsien agt 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:

2.7.1 Verantwoordingspligtigheid (*accountability*)
2.7.2 Beperkte prosessering (*processing limitation*)
2.7.3 Oogmerkspesifikasie (*purpose specific*)
2.7.4 Beperkte verdere prosessering (*further processing limitation*)
2.7.5 Inligtingsgehalte (*information quality*)
2.7.6 Openheid (*openness*)
2.7.7 Veiligheidsvoorsorgmaatreëls (*security safeguards*)
2.7.8 Deelname deur “datasubjek”

Voorwaarde 1: Verantwoordingspligtigheid

1. POPIA-Inligtingsbeampte

1.1 Elke Sinode of kerklike instansie moet ’n Inligtingsbeampte aanstel soos uiteengesit in die Wet, Artikel 55.
1.2 Die verantwoordelikhede van so ’n Inligtingsbeampte sluit die volgende in:
1.2.1 aanmoediging tot voldoening, deur die instansie, aan die voorwaardes vir die regmatige prosessering van persoonlike inligting;
1.2.2 die hantering van versoeke wat ooreenkomstig hierdie Wet aan die liggaam gerig word;
1.2.3 om met die Reguleerder saam te werk in verband met ondersoeke wat in ooreenstemming met Hoofstuk 6, met betrekking tot die instansie gedoen word;
1.2.4 om andersins, voldoening deur die instansie aan die bepalings van hierdie Wet te verseker en
1.2.5 soos wat voorgeskryf mag word.

1.3 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.

1.4 Naas die Wet (Artikel 55) moet die Inligtingsbeampte ook aan die volgende bykomende vereistes voldoen (Regulasie in Staatskoerant van 14 Desember 2018):

1.4.1 'n voldoeningsraamwerk ontwikkel, implementeer, monitor en onderhou;

1.4.2 'n persoonlike inligtingsimpak-assessering doen om te verseker dat voldoende maatreëls en standaarde bestaan ten einde te voldoen aan die voorwaardes vir die wettige verwerking van persoonlike inligting;

1.4.3 'n handleiding ontwikkel, moniteer, onderhou en beskikbaar stel soos in Artikel 11 en 51 van die Wet op die Bevordering van Toegang tot Inligting, Wet 2 van 2000, voorskryf;

1.4.4 interne maatreëls ontwikkel saam met voldoende stelsels om versoeke om inligting of toegang te verwerk en

1.4.5 interne bewusmaking sessies hou oor die bepalings van die Wet, regulasies ingevolge die Wet wat uitgevaardig is, gedragskode of inligting wat van die Reguleerder verkry is.

1.5 Diensgroepe en taakspanne moet 'n Adjunkinligtingsbeampte vir die taakspan aanwys welke Adjunkinligtingsbeampte onder toesig van die Hoofinligtingsbeampte werk. Hierdie Adjunkinligtingsbeampte:

1.5.1 is waarskynlik die taakspan se personeellid wat gemoeid is met al die data en inligting wat in die taakspan ingesamel, geberg en gebruik word;

1.5.2 het nie spesifieke kwalifikasies en/of opleiding vir hierdie taak nodig nie en

1.5.3 moet hom/haar gewis van die bepalings van die Wet soos uiteengesit in hierdie handleiding.

2. POPIA prosedure handleiding

2.1 Die Hoofinligtingsbeampte moet 'n prosedure handleiding saamstel wat aan die vereistes van die Wet voldoen. Die Sinodale Taakspan vir die Argief moet hierdie handleiding goedkeur.

2.2 Hierdie handleiding het ten doel om die NG Kerk in SA se beleid ten opsigte van die versekering van privaatheid te bepaal.

2.3 Die handleiding moet die volgende bevat:

2.3.1 Data insameling
- 2.3.1.1 Tipe data
- 2.3.1.2 Doel waarvoor die data ingesamel word
- 2.3.1.3 Toestemming van datasubjek (datasubjekte)
- 2.3.1.4 Berging van data
- 2.3.1.5 Deursigtigheid
- 2.3.1.6 Toegang tot data

2.3.2 Data gebruik en beperkings

2.3.3 Data berging

2.3.4 Data beveiliging

2.3.5 Data retensie

2.3.6 Data vernietiging

2.3.7 Personeel bewusmaking opleiding

2.3.8. Publisering van die handleiding

2.4 Wat betref die data van die datasubjek moet die volgende aandag kry:

2.4.1 **Insameling**: Die verskillende tipe inligting wat versamel gaan word, moet omskryf word.

2.4.2 **Beveiliging**: Omskryf hoe die data beveilig sal word in terme van fisiese en elektroniese sekuriteit.

2.4.3 **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 taakspan. Dit moet ook duidelik gestel word dat geen data aan ongemagtigde persone beskikbaar gestel sal word nie.

2.4.4 **Berging**: ’n Omskrywing van hoe en waar die data geberg gaan word.

2.4.5 **Retensie**: Hoe lank die data geberg word.

2.4.6 **Vernietiging**: Volledige beskrywing hoe die onbenutte en/of verouderde data vernietig gaan word.

2.5 Die Taakspan moet in oorleg met die Hoofinligtingsbeampte ’n inligtingsbeleid en prosedure handleiding vir gebruik in die taakspan saamstel.

2.6 Die Taakspan se inligtingsbeleid en prosedure handleiding moet die volgende bevat:

2.6.1 Welke persoon verantwoordelik is vir die insameling, bewaring en gebruik van datasubjekte se inligting.

2.6.2 Watter inligting versamel, geberg en gebruik word.

2.6.3 Hantering van inligting wat bepaal:

- 2.6.3.1 Op welke wyse die instemming van datasubjekte verkry is om die inligting te versamel, te berg en te gebruik.
- 2.6.3.2 Hoe toestemming van ouers verkry word wanneer inligting van minderjariges hanteer word.
- 2.6.3.3 Wysigings van inligting verkry vanaf die datasubjekte.

2.6.4 Metodes wat gebruik word om inligting te berg:

- 2.6.4.1 Skriftelike data
- 2.6.4.2 Elektroniese data

2.6.5 Metodes om inligting te beveilig:

- 2.6.5.1 Skriftelike data (bewaar byvoorbeeld in kluis)
- 2.6.5.2 Elektroniese data: wagwoorde, rugsteun, ensovoorts

2.6.6 Tydperk vir bewaring van inligting:

- 2.6.6.1 Watter inligting word hoe lank geberg
- 2.6.6.2 Hoe inligting geargiveer word

2.6.7 Vernietiging van inligting:

- 2.6.7.1 Skriftelike data (byvoorbeeld versnippering)
- 2.6.7.2 Elektroniese data wat uitgewis word

2.6.8 Gebruik van inligting:

- 2.6.8.1 Waarvoor word watter inligting gebruik
- 2.6.8.2 Doelspesifieke data vir sekere ampte, byvoorbeeld: watter salaris verdien die Predikante in Sinodale Diens, taakspanlede en administratiewe personeel.

2.7 Sodra die Adjunkinligtingsbeampte die inligtingsbeleid en prosedure handleiding vir die taakspan 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.

Voorwaarde 2: Beperkte prosessering

1. Persoonlike inligting moet

1.1 regmatig en

1.2 op ’n redelike wyse wat nie op die privaatheid van die datasubjek inbreuk maak nie, geprosesseer word.

2. Persoonlike inligting kan slegs geprosesseer word indien

2.1 ’n bevoegde persoon daartoe toestem;

2.2 direk van die datasubjek ingesamel is;

2.3 in die geval van minderjarige kinders, ’n bevoegde persoon (ouer/voog) toestemming verleen het;

2.4 noodsaaklik is vir die uitvoering van ’n handeling en

3.5 die regmatige belang van die datasubjek beskerm word.

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

4. Die diensgroep / taakspan moet

4.1 ’n Proses bepaal hoe:

4.1.1 bestaande datasubjekte se toestemming verkry behoort te word dat hulle inligting, versamel en geberg word;

4.1.2 toestemming moet ook verkry word dat hierdie inligting van datasubjekte gebruik mag word. Voorbeelde van hoe die inligting gebruik kan word, moet verskaf word;

4.1.3 wyse waarop ouer/voogde toestemming gee dat minderjariges se inligting versamel, geberg en gebruik mag word;

4.1.4 nuwe datasubjekte moet ook toestemming verleen dat hulle inligting versamel, geberg en gebruik mag word;

4.1.5 datasubjekte moet ook ingelig word van die wyse waarop hulle

- 4.1.5.1 inligting gewysig kan word
- 4.1.5.2 die Taakspan / Diensgroep / NG Kerk in SA versoek kan word om nie meer inligting te ontvang nie deur:
  - (a) skriftelik kennis te gee
  - (b) ’n uitteken opsie (*opt-out* funksie)

4.2 Bepaal hoe dikwels die inligting opgedateer moet word.

Voorwaarde 3: Oogmerkspesifikasie

1. Doel

1.1 Persoonlike inligting moet vir ’n bepaalde, uitdruklike omskrewe en regmatige oogmerk wat verband hou met die werksaamhede of aktiwiteite van die taakspan, diensgroep of NG Kerk in SA, ingesamel word.

2. Die handleiding moet die volgende omskryf:

2.1 **Watter** inligting benodig word.

2.2 **Hoe** die inligting bygewerk word wat verander.

2.3 Geloof- en filosofiese oortuigings

2.3.1 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.

2.3.2 Magtiging met betrekking tot datasubjek se geloof- of filosofiese oortuigings:

Artikel 28

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

(a) geestelike of geloofsverenigings of onafhanklike afdelings van daardie verenigings indien –

(i) die inligting betrekking het op datasubjekte wat aan daardie verenigings behoort; of

(ii) dit noodsaaklik is om hul oogmerke en beginsels te bereik

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

2.4 Die taakspan of diensgroep moet die volgende bepaal ten opsigte van:

2.4.1 Watter inligting van datasubjekte ingesamel gaan word soos byvoorbeeld:

2.4.1.1 persoonlike inligting, byvoorbeeld: volle name, van, geboortedatum en identiteitsnommer

2.4.1.2 adresbesonderhede, byvoorbeeld: woon- en posadres

2.4.1.3 kontakbesonderhede, byvoorbeeld: telefoonnommers, selfoonnommers en epos-adresse

2.4.1.4 ander inligting, byvoorbeeld: geslag, taalvoorkeur en beroep

2.4.1.5 finansiële inligting, byvoorbeeld: bankbesonderhede

2.4.2 Bepaling van doeleindes waarvoor die inligting gebruik gaan word.

Voorwaarde 4: Beperkte verdere prosessering

1. Toegang

1.1 Die diensgroep / taakspan moet bepaal watter personeel/datasubjekte toegang tot watter persoonlike inligting mag verkry.

1.1.1 Predikante in Sinodale Diens

1.1.1.1 Dit is noodsaaklik dat Predikante in Sinodale Diens en Bestuurders die minimum data van datasubjekte tot hulle beskikking het om hulle werk te kan verrig.

1.1.1.2 Dit kan in harde kopie of in elektroniese formaat 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 ’n genommerde kopie is wat weer later terugbesorg kan word vir vernietiging. Indien dit elektronies beskikbaar gestel word, moet daar verkieslik ’n wagwoord gegee word om toegang te verkry.

1.1.2 Diensgroep- of taakspanpersoneel

1.1.2.1 Administratiewe en finansiële personeel van die diensgroep of taakspan behoort toegang tot datasubjekte se inligting te verkry en te kan prosesseer. Sekere personeellede kan toegang tot die inligting verkry, 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.

1.1.2.2 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.

1.1.3 Taakspanlede

1.1.3.1 Taakspanlede 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.

1.1.3.2 Taakspanlede moet ontvangs erken vir alle persoonlike inligting wat hulle van die diensgroep ontvang vir kerklike gebruik.

1.1.4 Diensverskaffers / vennote

1.1.4.1 Vir diensverskaffers en vennote is dit ook noodsaaklik dat hulle oor bepaalde inligting moet beskik om hulle werk te verrig.

1.1.4.2 Diensverskaffers en vennote moet ontvangs erken vir alle persoonlike inligting wat hulle van die diensgroep ontvang vir kerklike gebruik alleenlik.

1.2 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.

2. Die diensgroep / taakspan moet bepaal wie toegang tot watter inligting het

2.1 Inligting wat benodig word vir administratiewe doeleindes.

2.2 Inligting wat deur die kantoor gebruik word vir byvoorbeeld nuusbriewe, verjaarsdae, SMS'e en ander kommunikasie met datasubjekte.

2.3 Inligting wat aan Predikant in Sinodale Diens voorsien moet word.

2.4 Inligting wat tot beskikking van sekere taakspanlede of personeel gestel moet word.

Voorwaarde 5: Inligtingsgehalte

1. Akkuraat

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

1.2 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 (byvoorbeeld naam, van en geboortedatum) en ander inligting wat meermale kan verander (adres, kontakbesonderhede, ensovoorts).

2. Prosedure

2.1 Die Diensgroep/Taakspan moet bepaal/sorg:

2.1.1 hoe die inligting op datum gehou word

2.1.2 gereeld 'n oudit doen om te bepaal hoe volledig en relevant (op datum) die inligting is.

2.1.3 In die oudit moet bepaal word:

- 2.1.3.1 watter inligting byna nooit verander nie, byvoorbeeld persoonlike besonderhede.
- 2.1.3.2 watter inligting per geleentheid verander, byvoorbeeld nooiensvan en kontakbesonderhede.
- 2.1.3.3 watter inligting gereeld nagegaan moet word wat dikwels verander, byvoorbeeld kontakbesonderhede soos telefoonnommers.

Voorwaarde 6: Openheid

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

2. Die verantwoordelike party (NG Kerk in SA) moet sorg dra vir die volgende:

2.1 die datasubjek moet bewus wees van die feit dat sy/haar inligting ingesamel word;

2.2 wie die inligting insamel (dus die naam en adres van die NG Kerk in SA, diensgroep of taakspan);

2.3 doel waarvoor die inligting ingesamel word en

2.4 hoe die inligting aangewend gaan word.

3. Die Diensgroep/Taakspan moet datasubjekte inlig:

3.1 dat hulle inligting versamel, geberg en gebruik word en

3.2 waarvoor die verskillende “vlakke” van inligting gebruik gaan word.

Voorwaarde 7: Veiligheidsvoorsorgmaatreël

1. Aldus Artikel 19 van die Wet is die NG Kerk in SA en sy gevolmagtigdes verantwoordelik vir die veiligheidsmaatreëls om die integriteit en vertroulikheid van persoonlike inligting te waarborg.

Artikel 19

(1) ’n Verantwoordelike party moet die integriteit en vertroulikheid van persoonlike inligting in die verantwoordelike party se besit of onder die verantwoordelike party se beheer beveilig deur geskikte, redelike tegniese en organisatoriese maatreëls daar te stel om –

(a) verlies van, skade aan, of ongemagtigde vernietiging van persoonlike inligting; en

(b) onregmatige toegang tot of prosessering van persoonlike inligting, te voorkom.

(2) Ten einde aan Subartikel (1) gevolg te gee, moet die verantwoordelike partyredelike maatreëls daarstel om –

(a) alle redelik voorsienbare interne en eksterne risiko’s ten opsigte van persoonlike inligting in die verantwoordelike party se besit of onder die verantwoordelike party se beheer, te identifiseer;

(b) geskikte voorsorgmaatreëls teen die geïdentifiseerde risiko’s in te stel en te onderhou;

(c) gereeld te kontroleer dat die voorsorgmaatreëls effektief geïmplementeer is; en

(d) te verseker dat die voorsorgmaatreëls voortdurend in reaksie op nuwe risiko’s of gebreke in vorige geïmplementeerde voorsorgmaatreëls opgedateer word.

(3) Die verantwoordelike party moet behoorlik ag slaan op algemeen aanvaarde inligtingsveiligheidspraktyke en prosedures wat van toepassing kan wees op ’n verantwoordelike party hetsy in die algemeen of wat ingevolge bepaalde bedryf- of professionele reëls en regulasies vereis kan word.

2. Die Diensgroep/Taakspan moet toesien dat die volgende vier aspekte in plek is:

2.1 **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 formaat of papier kopie bepaal ook die berging van die inligting. Persoonlike inligting word hoofsaaklik op die volgende wyses geberg:

2.1.1 Papier weergawes van inligting: Wanneer daar papier weergawes van persoonlike inligting gehou word, moet dit in ’n kluis weggesluit word.

2.1.2 Elektroniese weergawes op e-stelsels: diensgroepe, taakspanne en personeel wat persoonlike data invoer op stelsels soos databasisse moet bepaal op watter toestelle hierdie sagteware beskikbaar is (byvoorbeeld 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 2.1.3)

2.1.3 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.

2.1.4 E-posadresse: E-posadresse wat op rekenaarstelsels geberg word, kan op verskillende maniere geberg word, byvoorbeeld lokaal op die hardeskyf of op die Wolk met byvoorbeeld Outlook of Gmail. Daar moet toegesien word dat dit beveilig is teen ongemagtigde toegang.

2.1.5 Webwerf: Webwerwe verskaf dikwels persoonlike inligting oor personeel en vrywilligers. 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.

2.1.6 Sosiale media: Soos met webwerwe geld dieselfde reëls vir die plaas van persoonlike inligting op Facebook, Twitter, Instagram en enige ander sosiale media.

2.1.7 Selfone: Taakspanne en kollegas skep dikwels WhatsApp-groepe op selfone vir groepkommunikasie. 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 groeplede. Die datasubjek moet die opsie hê om die groep te kan verlaat.

2.1.8 Elektroniese Kommunikasie: Diensgroepe of taakspanne of personeel stuur dikwels kennisgewings aan betrokkenes. Daar moet skriftelike toestemming van die ontvanger 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 datasubjek kan onttrek.

2.2 Beveiliging

2.2.1 Die Oudit- en Risikokomitee van die NG Kerk in SA, Diensgroepe en Taakspanne moet aandag gee aan die fisiese en elektroniese beveiliging van persoonlike inligting.

2.2.2 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:

- 2.2.2.1 **Kluis** wat verkieslik ’n instapkluis is wat groot genoeg is om registers en ook rekenaartoerusting in te berg.
- 2.2.2.2 **Diefwering** voor alle vensters en deure wat na buite oopmaak.
- 2.2.2.3 **Alarmstelsel** wat verkieslik ’n alarmstelsel is wat gekoppel is aan ’n reaksie-eenheid.
- 2.2.2.4 **Sekuriteitskameras** waarmee toegang tot die terrein en gebou gemonitor kan word.
- 2.2.2.5 **Van-terrein beveiliging**: Maak seker dat die volgende in plek is:

(a) Rekenaar hardeskywe (eksterne) en geheuestokkies moet veilig gestoor word en
(b) Skootrekenaars moet veilig bewaar word.

2.2.3 Elektroniese sekuriteit: Ten opsigte van die elektroniese sekuriteit is daar drie belangrike sake naamlik: rugsteun, wagwoorde en enkripsie.

2.2.3.1 **Rugsteun**

(a) Rugsteun gereeld data wat op rekenaarstelsels gestoor word.
(b) Bewaar rugsteun wat op eksterne hardeskywe gedoen word op ’n veilige plek. Dit is sterk aan te raai dat dit op ’n ander plek as die kantoor gehou sal word.

2.2.3.2 **Wagwoorde**

(a) Gebruik sterk wagwoorde.
(b) Verander wagwoorde gereeld.
(c) Gebruik ’n wagwoord bestuurderprogram om al die verskillende wagwoorde van databasisse, webwerwe en stelsels te bestuur (byvoorbeeld KeePass).

2.2.3.3 **Enkripsie**

Sorg vir Antivirus-programme
Sorg vir Enkripsie-programme om dokumente te beskerm teen ongemagtigde toegang.

2.3 Data-retensie

2.3.1 Die Wet vereis dat inligting van datasubjekte nie langer geberg mag word as die oorspronklike oogmerk daarvan nie (Artikel 14 (1) en (2)). Raadpleeg hiervoor die Riglyne vir Bewaring soos deur die Argief van jaar tot jaar gepubliseer word. Die skakel daarheen is: https://www.kerkargief.co.za/doks/Tydperke.pdf

2.3.2 Die Wet bepaal egter dat inligting wel in sekere gevalle langer gebêre mag word, byvoorbeeld:

2.3.1.1 vir historiese, statistiese en navorsing doeleindes;
2.3.1.2 sekere finansiële inligting en
2.3.1.2 wanneer inligting benodig word vir die funksionering van die organisasie.

2.4 Vernietiging van data

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

2.4.1.1 Oorbodige duplikaat dokumente.
2.4.1.2 Duplikaat-uitdrukke wat as werkskopieë gebruik is.

2.4.2 Vernietiging moet met sorg geskied.

2.4.2.1 Elektroniese data (rekenaars, dataskywe en geheue stokkies)

(a) Ou rugsteundata moet vernietig word, sodat net die nuutste rugsteun beskikbaar is. Dit is goeie praktyk om weergawes te bestuur (*version control*).
(b) Vernietig elektroniese kopieë van inligting wat saamgestel is vir ’n ander doel, maar waarvan die oorspronklike inligting reeds in databasisse vasgevang is.
(c) Vernietig ou hardeskywe wat in onbruik is.

(d) 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.

2.4.2.2 Harde kopieë (papier rekords)

(a) Vermy om onnodige papier-uitdrukke van persoonlike data te maak.
(b) Moenie ongebruikte of ou inligtingstukke in die snippermandjie gooi nie.
(c) Sien toe dat dit verbrand, versnipper of verpulp word.

2.5 **Diefstal**

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

Voorwaarde 8: Deelname deur datasubjek

1. Die datasubjek het die reg om:

1.1 toegang te hê tot persoonlike inligting wat oor hom/haar gehou word en mag vra om toegang te verkry tot eie persoonlike inligting;

1.2 te versoek dat regstellings of skrapping gemaak word op eie persoonlike inligting en kan ook versoek dat rekords van persoonlike inligting vernietig word en

1.3 beswaar te maak teen die verwerking van persoonlike inligting.

2. Datasubjekte 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 verkry tot inligting.

3. Ten opsigte van **POPIA** is die volgende vorms beskikbaar op die webblad van die NG Kerk:

3.1 Beswaar teen verwerking van persoonlike inligting (Vorm 1)

3.2 Versoek om regstelling of skrapping van persoonlike inligting of vernietiging of skrapping van rekord van persoonlike inligting (Vorm 2)

3.3 Aansoek om die toestemming van ’n datasubjek vir die verwerking van persoonlike inligting vir die doel van direkte bemarking (vorm 4)

ALGEMENE BEPALINGS

1. Regsadvies

1.1 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 soos volg: “Kommunikasie tussen regsadviseur en kliënt vrygestel”.

Artikel 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".

2. Uitkontraktering

2.1 Die NG Kerk in SA sou ook met 'n onafhanklike operateur 'n kontrak kan sluit om as agent op te tree ingevolge die Wet.

2.2 'n Operateur word omskryf as "'n persoon wat ingevolge 'n kontrak of mandaat persoonlike inligting vir 'n verantwoordelike party (diensgroep / taakspan) prosesseer sonder om onder die direkte gesag van daardie party te wees". Die operateur is dus nie 'n werknemer nie, maar 'n derde party wat namens die NG Kerk in SA die take soos omskryf in POPIA uitvoer.

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

Inligting geprosesseer deur operateur of persoon wat kragtens magtiging optree
Artikel 20

(1) '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
Artikel 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.

2.4 Die NG Kerk in SA (of diensgroep of taakspan) sal in hulle skriftelike kontrak met die operateur moet toesien dat dit onder andere die volgende bepalings bevat:

2.4.1 sien toe dat aan die Wet voldoen word en spesifiek Artikel 19 – dat die veiligheidsvoorsorgmaatreëls getref word;

2.4.2 onmiddellik die verantwoordelike party inlig indien enige vereistes verbreek is;

2.4.3 vertroulike inligting beskerm word;

2.4.4 nie persoonlike inligting prosesseer sonder die magtiging of toestemming van die verantwoordelike party nie;

2.4.5 monitering en ouditering deur die verantwoordelike party om nakoming van die Wet deurgaans te verseker en

2.4.6 ’n vrywaring van die operateur vereis word, indien diensvoorwaardes verbreek sou word.

- o0o -